Maßnahmenkatalog der Österreichischen Strategie für Cybersicherheit 2021

Fortschrittsbericht 1/2025

Maßnahmenkatalog der Österreichischen Strategie für Cybersicherheit 2021

Fortschrittsbericht 1/2025

Wien, 2025

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundeskanzleramt, Ballhausplatz 2, 1010 Wien
Telefon: +43 1 531 15-123456
bundeskanzleramt.gv.at
Gestaltung: BKA Design & Grafik
Wien, 2025

Inhalt

Präambel

Mit der neuen Österreichischen Strategie für Cybersicherheit 2021 (ÖSCS 2021) wurde von der Bundesregierung am 22. Dezember 2021 ein erneuertes, umfassendes und proaktives Konzept zum Schutz des Cyberraums und der Menschen im virtuellen Raum beschlossen. Die ÖSCS 2021 bildet daher das Fundament der gesamtstaatlichen Zusammenarbeit in diesem Bereich. Sie wurde von Expertinnen und Experten aus den Bereichen Wirtschaft, Bildung, Forschung und Entwicklung, Verbindungspersonen zum Nationalen Sicherheitsrat sowie Expertinnen und Experten des Bundes in einem mehrstufigen Prozess unter Federführung des Bundeskanzleramtes erarbeitet. Die ÖSCS 2021 ist auf der Webseite des Bundeskanzleramtes verfügbar.

Aufbau der ÖSCS 2021

Die ÖSCS 2021 besteht aus zwei Teilen: einem strategischen Rahmenwerk und einem dynamischen, webseitengestützten Maßnahmenkatalog.

Der erste Teil, der strategische Überbau, umfasst die Erläuterung zur Ausgangslage, die Herausforderungen und die sich daraus ergebenden Chancen, den Rahmen für die Umsetzung sowie die Steuerungs- und Monitoringprozesse der Strategie.

Im zweiten Teil sind die konkreten Maßnahmen, die gesetzt werden, um die Ziele der Strategie zu erreichen, definiert. Das Monitoring der Strategieumsetzung sowie die Verwaltung und Sammlung der Maßnahmen erfolgt über eine Online-Plattform. Jede Maßnahme ist zumindest einem der in Kapitel 3 der ÖSCS 2021 genannten Ziele und einer oder mehrerer in Kapitel 4 der ÖSCS erwähnten Zielgruppen zuzuordnen. Somit kann flexibel auf sich ständig weiterentwickelnde Bedrohungslagen sowie aktuelle Herausforderungen reagiert und gleichzeitig die Abdeckung der Ziele der ÖSCS 2021 durch konkrete Maßnahmen festgestellt werden.

Fortschrittsmessung

Die Cyber Sicherheit Steuerungsgruppe (CSS) zeichnet sich für die Aktualisierung und die Fortschrittsmessung der Maßnahmen verantwortlich. In der ÖSCS 2021 verpflichtet sich die CSS, die Maßnahmen regelmäßig – soweit möglich – zu veröffentlichen.

Das vorliegende Dokument stellt einen Auszug aus dieser Monitoring-Plattform dar und spiegelt den Umsetzungsstatus der Ziele der ÖSCS 2021 mit Stichtag 5. März 2025 wider. Es werden die Projekte der jeweiligen Ressorts, welche die Maßnahmen zur Zielerreichung darstellen, aufgelistet. Die Fortschrittsmessung sowie der Status der Umsetzung veranschaulicht den Progress der Projekte im gesetzten Zeitraum – also Start und geplantes Ende der Projekte.

Neben der **Projektbezeichnung** werden **Gegenstand** und **Ziele** angeführt und der **Projektstatus** mit einer Beschreibung erläutert. Die **zugrundeliegenden strategischen Ziele** der Maßnahme beschreiben, welche der definierten Ziele der ÖSCS 2021 mit der Umsetzung der Maßnahme angestrebt werden. Unter **Herausforderungen** werden die Bedrohungen beschrieben, die in der Projektumsetzung besonders zu berücksichtigen sind. Eine schwerpunktmäßige Zuordnung der Maßnahme wird bei **Zielgruppe** und **Themenbereiche** gesetzt.

Nicht nur die Bundesministerien in ihrem eigenen Verantwortungsbereich, sondern auch die Privatwirtschaft, die Wissenschaft und die Gesellschaft haben über ihre Vertreterinnen und Vertreter Maßnahmen gegenüber der CSS bekannt gemacht. Somit wurde dem Anspruch eines gesamtstaatlichen Ansatzes Rechnung getragen.

Die aktuellen Maßnahmen werden in Zwischenschritten, die in einem Zeitabstand von einem halben Jahr erfolgen, einer Evaluierung durch die CSS unterzogen und der Fortschritt dokumentiert.

Bericht der Cyber Sicherheit Plattform

Cybersecurity Aktivitäten
Stand: 5.3.2025

Mit der ÖSCS 2021 wurde neben dem strategischen Dokument, welches unter anderem Vision, Ziele und Zielgruppen definiert, ein webbasierter dynamischer Maßnahmenkatalog erstellt.

In diesem werden die einzelnen Aktivitäten der Ministerien und Stakeholder aus den unterschiedlichen Bereichen gesammelt, verwaltet und der Fortschritt nachvollziehbar gemacht.

In regelmäßigen Abständen werden jene Maßnahmen, welche keinen Sicherheitseinschränkungen unterliegen, veröffentlicht.

Projektübersicht

Managementsummary über die Leuchtturmprojekte der Bundesregierung

Cybersecurity Aktivitäten

Stand: 5.3.2025

Ressort	Project	Start	Ende	Fortschritt / Projektampel
BKA	Aufbau NCC	27.6.2021	31.8.2025	90 %
BMLV	Ausbau und verstärkte EU-Koordinierung nationaler milCERTs (Beitrag zum CDPF-Review der EU)	9.9.2021	31.12.2026	40 %
BMI	Ausbau des Computer Security Incident Response Teams des BMI (CSIRT-BMI)	31.8.2020	2.5.2023	100 %
BMEIA	Einsetzung Sonderbeauftragter für Cyber-Außenpolitik und Cyber-Sicherheit	30.4.2021	1.5.2021	100 %
BMEIA	Einrichtung Referat Cyberdiplomatie, sicherheitspolitische Aspekte neuer Technologien	1.9.2020	1.7.2021	100 %
BMEIA	Verhandlungen VN-Cybercrimekonvention: Bereitstellung Junior Professional Officer für UNODC	31.8.2021	31.12.2024	100 %
BMEIA	VN-Cybercrimekonvention: Reisekostenzuschuss für LDCs, LLDC, SIDS	25.4.2021	31.12.2023	100 %
CSP/PPP	A1 Seniorenakademie	31.3.2021	31.12.2099	100 %
BMEIA	Teilnahme an Forschungs- und Entwicklungsprojekten	31.8.2021	30.4.2025	95 %
BMBWF	Förderung der Cybersicherheit durch Pflichtfach Digitale Grundbildung	1.10.2021	6.7.2022	100 %
BMJ	Einrichtung von Cybercrime Kompetenzstellen an Staatsanwaltschaften	1.10.2022	29.6.2023	100 %
BMAW	[BEV] Zusätzliche Ressourcen für den Schutz der kritischen Infrastruktur	1.1.2021	31.12.2023	
BMAW	[BEV] GAP-Analyse zur Informationssicherheit	18.9.2021	31.12.2023	1 %
BMAW	[Sektion VI] Cybersicherheit in der dualen Berufsausbildung	1.12.2020	31.12.2023	100 %
BMAW	[PRÄS] Konzept für Cybersicherheits-Berichtswesen (IKT-W)	1.1.2022	31.5.2024	100 %
BMAW	[PRÄS] Überprüfung der IT-Sicherheitsmechanismen 2021 für den BMDW-Standardarbeitsplatz (IKT-W)	20.1.2023	28.4.2022	100 %
BMAW	[PRÄS] Etablierung einer IT-Notfall-Organisation (IKT-W)	29.7.2021	27.6.2022	100 %
BMAW	[Sektion IV] Förderungsprogramm „KMU.Cybersecurity“	1.4.2022	30.4.2024	100 %
BMSGPK	IT-System zur Erkennung von sicherheitskritischen Ereignissen (SIEM) gemäß Etappenplan	1.2.2023	31.12.2025	85 %
BMSGPK	Etablierung Leitlinien Risikomgmt. in der Netz- und Informationssicherheit	1.2.2023	20.12.2024	100 %
BMSGPK	Weiterentwicklung des Informationssicherheitsmanagement (ISMS) Tools	1.2.2023	31.12.2025	80 %
BMAW	[PRÄS] Aktualisierung der InfoSih-Richtlinie (IKT-W)	30.4.2023	31.5.2024	100 %
BMAW	[PRÄS] Überprüfung der IT-Sicherheitsmechanismen 2023 (IKT-W)	1.6.2023	29.2.2024	100 %
BMLV	Erstellung eines Querschnittskonzepts „Einsatz im Cyber-Raum“	3.7.2022	31.12.2023	100 %

Ressort	Project	Start	Ende	Fortschritt / Projektampel
BMLV	Umsetzung der EU Cyber Defence Policy	10.7.2023	31.12.2028	25%
Regulatoren	E-Control Energie-Branchenrisikoanalyse	1.1.2024	31.3.2025	90%
BKA	Vorantreiben Einrichtung Cyber Rapid Response Teams	21.2.2024	1.1.2099	50%
Regulatoren	FMA – Assessment der Mitigationsmaßnahmen	1.1.2024	31.12.2099	60%
Regulatoren	FMA – DORA-Gap-Analyse	1.1.2024	31.12.2099	60%
Regulatoren	FMA – DORA-Beaufsichtigung	8.2.2024	31.12.2099	100%
Regulatoren	FMA – IT Governance Einsichtnahmen	30.9.2023	31.12.2099	100%
BMSGPK	Erstellung eines Maßnahmenplans zur Netz- und Informationssicherheit	1.1.2024	30.6.2025	80%
BMI	Betrieb von IKT-Lösungen zur frühzeitigen Erkennung von Risiken oder Vorfällen in NIS	31.7.2022	29.9.2027	46%
BMLV	Erstellung eines umfassenden militärischen Cyber-Lagebildes	1.1.2024	31.12.2028	15%
BMLV	Aufbau einer militärischen Cyber Range	31.3.2021	31.12.2024	15%
BMLV	Aufbau von Cyber Rapid Response Teams (CRRT) im BMLV	31.3.2024	31.12.2024	40%
BMLV	Bereitstellung einer KI Risikoanalyse für einsatzrelevante IKT Systeme des ÖBH	1.12.2024	31.12.2025	10%
BMLV	Gezielte Förderung von Innovation im Cyber-Raum durch konkrete Maßnahmen	30.6.2024	31.12.2026	10%
CSP/PPP	AIT – Fake Shop Detector (FSD)	1.1.2024	24.12.2026	60%
CSP/PPP	AIT – Kampf gegen Desinformation	1.1.2024	24.12.2026	60%
CSP/PPP	OeNB – Off-Site Analyse bei österreichischen LSI	30.11.2017	31.12.2099	100%
CSP/PPP	OeNB – DORA-Implementierung für die LSI Off-Site Analyse	1.7.2024	31.12.2026	65%
CSP/PPP	FH JOANNEUM – TRANSFORM	1.1.2024	30.8.2025	80%
CSP/PPP	SBA Security Advisories	1.1.2020	31.12.2099	100%
BMF	1. Ausschreibung: Kybernet-Pass (K-PASS)	30.10.2023	1.3.2024	100%
BMEIA	Mitwirkung und Outreach in der International Counter Ransomware Initiative (CRI)	29.10.2021	31.12.2099	60%
BKA	Aufbau Nationale Cybersicherheitszertifizierungsbehörde (NCZB)	1.3.2024	31.12.2025	80%
BMAW	[PRÄS] Überprüfung der IT-Sicherheitsmechanismen 2024 für den BMAW-Standardarbeitsplatz (IKT-W)	1.11.2024	28.2.2025	100%
BKA	Vorbereitung Umsetzung Cyber Resilience Act (CRA)	1.2.2025	31.12.2027	5%
BKA	Implementierung der CVD Plattform und Meldeprozesse gem. NIS2-RL	5.2.2025	31.12.2025	15%
BKA	Standardisierte/gemeinsame Ausbildung der CISOs in den Bundes-ministerien	31.5.2024	31.5.2025	70%
CSP/PPP	FH OÖ F&E GmbH – Cybersecurity Forschung	1.10.2009	31.12.2099	100%
CSP/PPP	FH JOANNEUM – Go Cloud Go Secure	1.11.2024	30.10.2026	10%
CSP/PPP	FH JOANNEUM – RADIUS	1.1.2025	31.12.2029	5%
BKA	Förderung von Projekten zur Stärkung von Frauen und Mädchen im digitalen Raum	1.10.2023	31.12.2025	60%

Ressort	Project	Start	Ende	Fortschritt / Projektampel
BMEIA	Engagement in der OSZE für Public-Private Partnerships als VBM	1.1.2018	31.12.2099	10 %
BMEIA	Engagement gegen den Missbrauch von kommerziellen Cyber-Intrusion-Tools	22.9.2024	31.12.2099	5 %
BMEIA	VN Cybercrime-Konvention: Unterzeichnung/Ratifizierung/Umsetzung	24.12.2024	31.12.2028	5 %
CSP/PPP	OeNB, FMA – TIBER-AT Implementation	1.8.2024	30.9.2025	85 %
CSP/PPP	AIT – KI-basierte Technologien für effektive Cyber Security Schutzmaßnahmen	1.1.2024	31.12.2026	60 %
CSP/PPP	AIT/GAIA-X – wiki.ATLAWS.eu	1.1.2024	31.12.2026	80 %
CSP/PPP	AIT – Internationales Digital Security Forum (IDSF)	1.1.2023	31.12.2027	80 %
CSP/PPP	AIT/KSÖ – nationales Cyber Security Planspiel mit Behörden und KRITIS	1.1.2023	31.12.2027	80 %
Regulatoren	E-Control – Umsetzung Network Code Cyber Security	12.6.2024	31.12.2028	5 %
Regulatoren	E-Control: Gemeinsame Übung Cyber Europe	18.6.2024	20.6.2024	100 %
BMI	Ausbau C 4 zu moderner High Tech Einheit	1.1.2021	30.6.2025	80 %
Regulatoren	FMA – Cyber Maturity Level Assessment	1.1.2022	31.12.2099	70 %
BKA	Umsetzung NIS 2 Richtlinie	16.1.2023	31.10.2025	80 %
CSP/PPP	A1 Seniorenakademie in A1 Shops	1.1.2023	31.12.2099	100 %
BKA	Etablierung CISO in den Bundesministerien	15.12.2020	31.12.2023	100 %
BMI	Umsetzung und/oder funktionelle Erweiterungen der IKT-Lösungen gem. NISG	1.1.2021	30.9.2027	100 %
CSP/PPP	A1 digital.campus	1.1.2020	31.12.2099	100 %
Regulatoren	FMA, OeNB – Vor-Ort-Prüfungen bei den beaufsichtigten Finanzunternehmen	30.6.2018	31.12.2099	100 %
BKA	Sicherheitsstandards gem. NISG im öffentl. Sektor	15.12.2020	31.12.2024	90 %
BMI	ÖSCS 2021	16.8.2021	29.9.2023	100 %
BMLV	Intensivierung der internationalen Kooperation zur besseren Beitragsleistung bei Cyber-Vorfällen	20.3.2013	1.1.2026	60 %
Regulatoren	FMA – Blackout Maturity Level Assessment	20.1.2022	31.12.2099	80 %
CSP/PPP	A1 digital.campus – MINT & Engineering Fokus	19.2.2024	31.12.2099	10 %
BMI	Anpassung Cybercrime Delikte (Abstimmung mit BMJ)	31.8.2021	1.9.2023	100 %
BMLV	Nutzung von Cyber-Threat-Intel-Plattformen zur Verdichtung des Cyber-Lagebildes	2.1.2022	31.12.2027	90 %
Regulatoren	FMA – Cyber Security Exercise	1.1.2022	31.12.2099	60 %
CSP/PPP	Uni Wien – DaTra	1.12.2022	31.1.2024	100 %
BMI	Cyber Cops-Bezirks IT Ermittler	31.8.2021	30.9.2025	60 %
BMLV	Ausbau von Fähigkeiten zur Erkennung gezielter Manipulation des Informationsraums	1.1.2021	31.12.2031	55 %
Regulatoren	RTR – Hochrisikolieferanten	1.1.2022	31.12.2099	100 %
BKA	IT-Konsolidierungsprogramm: Security Framework Bund II – Anpassung an NIS 2	1.1.2024	31.5.2025	30 %

Ressort	Project	Start	Ende	Fortschritt / Projektampel
CSP/PPP	SBA – ASOC	1.1.2024	1.1.2026	30 %
BMLV	Ausbau von Fähigkeiten zur Netzwerkforensik- und Malwareanalyse sowie Reverse-Engineering	1.1.2021	31.12.2023	70 %
CSP/PPP	FMA,OENB – TIBER AT Framework	6.4.2021	31.12.2023	100 %
BMI	Betrieb einer Kollaborationsplattform für den IKDOK	31.8.2022	29.6.2024	100 %
BKA	Erstellen eines Cyberübungsframeworks	22.11.2022	31.3.2024	100 %
BKA	Aufbau NCCA	15.12.2020	31.12.2025	90 %
BMLV	Beitrag zum gesamtstaatlichen Lagebild über den Weg des IKDOK	20.3.2013	1.1.2030	100 %
Regulatoren	RTR – 5G Sicherheit	1.1.2022	15.6.2022	100 %
BMI	Erlassung von Geschäftsordnungen für die Koordinierungsstrukturen	31.8.2022	29.12.2023	100 %
CSP/PPP	FMA, OeNB – Threat Led Penetration Testing	1.1.2023	31.12.2099	85 %
CSP/PPP	KSÖ – Baseline Cybersecurity Standard für KMUs	27.1.2021	31.3.2023	60 %
Regulatoren	RTR – Informationssicherheitsmanagement und Sicherheitsstandards	1.1.2022	15.6.2022	100 %
BMI	Erstellung von standardisierten Vorgehensweisen (SOPs) für die Koordinierungsstrukturen	1.9.2022	31.3.2024	100 %
BKA	NCC-Förderung: Cyber Security Schecks	31.7.2023	31.8.2025	90 %
CSP/PPP	FH OÖ – Fachhochschulausbildung in Informationssicherheit	31.8.2000	31.12.2099	100 %
Regulatoren	RTR – TK-Branchenrisikoanalyse (TK-BRA)	1.1.2022	15.6.2022	100 %
BMI	Erstmaßnahmen bei Cybersicherheitsvorfällen	1.7.2022	31.12.2024	100 %
BKA	BKA – Förderungen von Projekten mit Schwerpunkt auf Bekämpfung von Cyber-Gewalt	1.11.2022	31.12.2023	100 %
BMLV	Erstellung einer Cyberverteidigungsstrategie und Fähigkeitenprofils zur Cyberverteidigung	1.2.2021	31.12.2023	100 %
CSP/PPP	WKÖ – IT-SAFE	1.1.2022	31.12.2099	100 %
Regulatoren	RTR – TK Cybersecurity Expertengruppe	1.1.2022	1.1.2099	100 %
BMI	Schaffung einer IKT Lösung für besondere kriminalpolizeiliche Ermittlungen	18.3.2021	31.12.2025	60 %
BKA	Förderung von Fortbildungsseminaren zum Thema Cyber-Gewalt in (Ex-) Paarbeziehungen	1.4.2023	31.3.2025	95 %
BKA	Ausbau des Zentralen Ausweichsystem des Bundes im Rahmen der Digitalen Arche	19.11.2021	1.1.2025	45 %
BMLV	Stärkung der Cybersicherheit durch Schutz der eigenen IKT-Systeme	12.10.2020	31.12.2026	40 %
CSP/PPP	WKÖ – CYBER SECURITY HOTLINE WKO	1.1.2022	31.12.2099	100 %
Regulatoren	RTR – Behördentreffen IT-Risiko	1.1.2022	31.12.2099	100 %
BKA	Erhöhung der Cybersicherheit im BKA	2.11.2021	31.12.2025	95 %
CSP/PPP	WKÖ – CYBER SECURITY FEUERWEHR WKO	1.1.2022	31.12.2099	20 %
Regulatoren	RTR – Mustersicherheitskonzept	1.1.2022	15.6.2026	10 %
BMLV	Fokus auf technische Entwicklungen (Digitalisierung) in der Streitkräfteplanung und -entwicklung	26.9.2017	26.9.2032	40 %
Regulatoren	RTR – Vernetzung mit E-Wirtschaft	1.1.2022	31.12.2099	100 %

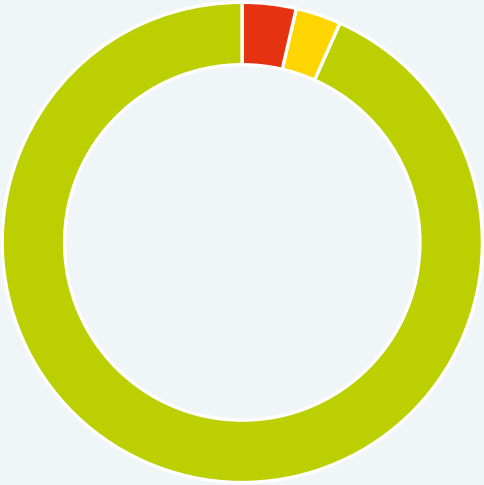
Ressort	Project	Start	Ende	Fortschritt / Projektampel
CSP/PPP	WKÖ – Women4Cyber Austria	31.8.2022	31.12.2099	100 %
BMLV	Verankerung der Cyber-Domäne im MSK und Aufbau von Cyber-Kräften im ÖBH	25.9.2017	26.9.2032	60 %
CSP/PPP	VERBUND – OT Cyber Security Lab	14.6.2020	31.12.2023	100 %
BMLV	Bereitstellung von OpenSource-Information durch das CyDok&ForschZ (Recherche und Analyse)	1.1.2014	31.12.2024	100 %
CSP/PPP	COMPARO – OPSAM Community Edition: zentrale Wissensdrehscheibe Cybersicherheit	30.9.2021	31.12.2025	100 %
BMLV	Einführung des FH-Bachelorstudiengangs „Militärische IKT-Führung“ an der TherMilAk	31.8.2022	31.12.2023	100 %
CSP/PPP	DVC – Trainingskurs OPCYBRES: Cybersicherheit als Eckpfeiler der Unternehmensresilienz	1.11.2021	31.12.2099	100 %
BMLV	Neugestaltung der ADV-Sonderverträge für IT-Personal (FF BMKÖS)	1.1.2021	31.12.2026	80 %
CSP/PPP	KPMG/KSÖ-Cybersicherheitsstudie „Cybersecurity in Österreich“	1.8.2024	30.6.2025	20 %
CSP/PPP	KPMG – Cyber Awareness Monat Oktober 2024: Sensibilisierung und Trainings	31.5.2024	31.12.2024	40 %
CSP/PPP	INDUCE Cyber Security Literacy And Dexterity through Cyber Exercises	1.4.2021	31.3.2024	30 %
CSP/PPP	AIT – Post-Quanten-Computer sichere Verschlüsselung für höchste Cyber Sicherheit	1.1.2021	31.12.2026	70 %
CSP/PPP	AIT – Ausbau der Cyber-Security Widerstandsfähigkeit für kritische Infrastrukturbetreiber in AT	1.1.2021	31.12.2026	95 %
CSP/PPP	Learners – effizientere Methodologien + Methodiken komplexe und Dynamische Inhalte für Jugend	1.4.2022	31.12.2023	4 %
CSP/PPP	Nationales Cyber Security Trainingszentrum	31.8.2022	31.12.2025	2 %
CSP/PPP	VISP – Vienna InternetSecurityPrivacy Cluster	1.3.2020	31.12.2099	100 %
CSP/PPP	OCG – Young Researchers Day	1.3.2024	31.12.2099	100 %
CSP/PPP	CSA – HackFu	30.9.2022	29.9.2023	15 %
CSP/PPP	„Shecurity“ – Hackerinnen Training	31.5.2023	31.12.2099	100 %
CSP/PPP	SBA, sec4dev – youTube Kanal	4.9.2015	31.12.2099	100 %
CSP/PPP	SBA, ÖIAT – Security Awareness Stammtisch	24.4.2023	31.12.2099	100 %
CSP/PPP	SBA – Cybersecurity Quiz	30.9.2021	31.12.2099	100 %
CSP/PPP	SBA – securepizza.club @ SBA Research	1.1.2021	31.12.2099	100 %
CSP/PPP	SBA – Women in Privacy & Security Vienna	1.1.2021	31.12.2099	100 %
CSP/PPP	SBA – Seurity Meetup	1.1.2021	31.12.2099	100 %
CSP/PPP	ISPA – Der Online-Zoo	1.12.2015	1.7.2025	75 %
CSP/PPP	ACSC – Austrian Cyber Security Challenge 2023	1.1.2023	31.12.2023	60 %
CSP/PPP	ECSC – European Cyber Security Challenge 2023	1.1.2023	31.12.2023	50 %
CSP/PPP	openECSC – Open European Cyber Security Challenge 2023	20.1.2023	31.12.2023	35 %
CSP/PPP	FH OÖ – SSCCS (Secure Supply Chains for critical systems)	30.6.2021	31.12.2024	80 %
CSP/PPP	FH OÖ – CySeReS-KMU	1.1.2023	30.6.2025	70 %

Ressort	Project	Start	Ende	Fortschritt / Projektampel
CSP/PPP	FH OÖ – Sucredi	1.1.2019	29.6.2022	100 %
CSP/PPP	AIT -Aufbau von Übungs- und Trainingsplattformen für Multistakeholder Infrastrukturszenarien	30.9.2022	31.12.2024	70 %
CSP/PPP	AIT – Realisierung von Cyber Security Schlüsseltechnologien made in Austria mit globalem Impact	1.1.2022	31.12.2025	90 %
CSP/PPP	AIT – Beitrag Österreichs zur Umsetzung des EU Cyber Resilience Acts	1.1.2022	31.12.2026	70 %
CSP/PPP	AIT – Aufbau effektiver Threat-Intelligence Fähigkeiten für den Wirtschaftsstandort Österreich	1.1.2022	31.12.2026	60 %
CSP/PPP	Mindsetters – Cyber-Awareness für Österreich – Produktname: „2b-aware“	31.7.2022	1.5.2024	100 %
CSP/PPP	AKNOe -Onlinebetrug-Simulator	1.7.2021	30.6.2022	100 %
CSP/PPP	epicenter.academy: Digitale Selbstverteidigung	12.12.2022	1.7.2028	50 %
CSP/PPP	AIT – Österreich als aktiver EU Cyber Security Skill Development Stakeholder	1.6.2023	31.12.2026	10 %
CSP/PPP	SV – Weiterentwicklung SV-Sicherheitsstandards	1.10.2022	31.3.2024	80 %
CSP/PPP	FH JOANNEUM – Masterstudium IT & Mobile Security	1.1.2001	31.12.2099	100 %
CSP/PPP	FH JOANNEUM – CyMoDACS: Cyber-Security and Mobility for Digital Aeronautic Communication Systems	1.1.2022	30.6.2025	80 %
CSP/PPP	FH JOANNEUM – CSecTOR	1.12.2022	30.11.2024	100 %

Auswertung für: Alle Ressorts

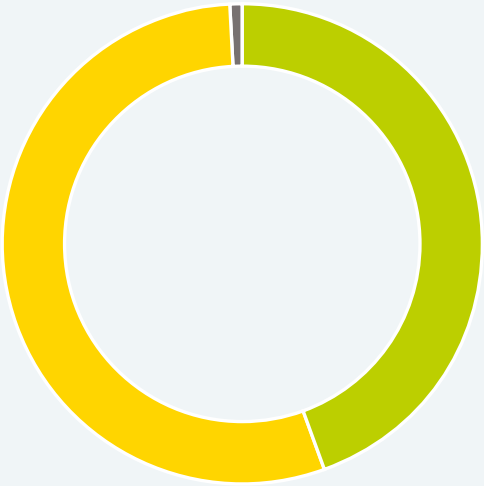
Statusindikator (Projektampel)

- Rot (Projekt gefährdet): 6
- Gelb (Projekt problembehaftet): 5
- Grün (Projekt nach Plan): 151



Umsetzungsstatus

- Abgeschlossen: 72
- In Arbeit: 89
- Geplant: 1



Fertigstellungsgrad

- Erfüllt: 73,85 %
- Nicht Erfüllt: 26,15 %

BKA

Projektverantwortliches Ressort
Bundeskanzleramt

Stand: 5.3.2025

Nr.	Projekt	Status	Fortschritt / Projektampel	Start	Ende
1	Aufbau NCC	grün	90 %	27.6.2021	31.8.2025
2	Vorantreiben Einrichtung Cyber Rapid Response Teams	grün	50 %	21.2.2024	1.1.2099
3	Aufbau Nationale Cybersicherheitszertifizierungsbehörde (NCZB)	grün	80 %	1.3.2024	31.12.2025
4	Vorbereitung Umsetzung Cyber Resilience Act (CRA)	grün	5 %	1.2.2025	31.12.2027
5	Implementierung der CVD Plattform und Meldeprozesse gem. NIS2-RL	grün	15 %	5.2.2025	31.12.2025
6	Standardisierte/gemeinsame Ausbildung der CISOs in den Bundesministerien	grün	70 %	31.5.2024	31.5.2025
7	Förderung von Projekten zur Stärkung von Frauen und Mädchen im digitalen Raum	grün	60 %	1.10.2023	31.12.2025
8	Umsetzung NIS 2 Richtlinie	gelb	80 %	16.1.2023	31.10.2025
9	Etablierung CISO in den Bundesministerien	grün	100 %	15.12.2020	31.12.2023
10	Sicherheitsstandards gem. NISG im öffentl. Sektor	grün	90 %	15.12.2020	31.12.2024
11	IT-Konsolidierungsprogramm: Security Framework Bund II – Anpassung an NIS 2	grün	30 %	1.1.2024	31.5.2025
12	Erstellen eines Cyberübungsframeworks	grün	100 %	22.11.2022	31.3.2024
13	Aufbau NCCA	grün	90 %	15.12.2020	31.12.2025
14	NCC-Förderung: Cyber Security Schecks	grün	90 %	31.7.2023	31.8.2025
15	BKA – Förderungen von Projekten mit Schwerpunkt auf Bekämpfung von Cyber-Gewalt	grün	100 %	1.11.2022	31.12.2023
16	Förderung von Fortbildungsseminaren zum Thema Cyber-Gewalt in (Ex-)Paarbeziehungen	grün	95 %	1.4.2023	31.3.2025
17	Ausbau des Zentralen Ausweichsystem des Bundes im Rahmen der Digitalen Arche	grün	45 %	19.11.2021	1.1.2025
18	Erhöhung der Cybersicherheit im BKA	grün	95 %	2.11.2021	31.12.2025

Projekt: Aufbau NCC

Start: 27.6.2021
Ende: 31.8.2025
Nr.: 1003

Aktuelles Jahr
Status: grün
Fortschritt: 90 %

Zugrundeliegende Strategische Ziele

– Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen
– Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
– In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit

Gegenstand und Ziele

Die EU-Verordnung zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren verpflichtet die Mitgliedstaaten, nationale Koordinierungszentren einzurichten. Die Aufgaben des NCC sind in Artikel 7 festgelegt, welche durch ein Aufbauprojekt im BKA entsprochen werden soll.

Beschreibung des Status

- Nach Ausarbeitung von Optionen zur Implementierung Entscheidung, NCC im BKA aufzubauen
- Umsetzung durch Trennung operative und strategische Aufgaben
- Vertragsabschluss mit Österreichischen Forschungsförderungsgesellschaft (FFG) als externer Dienstleister
- Eingeschränkte Operativsetzung erfolgt
- Aufbau interner Strukturen, inkl. initialer Personalaufstellung
- EU-Kofinanzierungsmittel aus dem EU-Finanzierungsprogramm „Digitales Europa“ für Aufbau und erste Förderinitiative für KMU angeworben
- EU-Projektabwicklung gestartet, inkl. feierliche Eröffnung und Operativsetzung
- Laufende Abwicklung EU-Projekt „NCC-AT“ durch BKA und FFG
- Entwicklung von Optionen zur nachhaltigen Verankerung des NCC-AT in Österreich nach EU-Projekt

Organisationsfeld

BKA I/8

Herausforderungen

Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Forschung & Entwicklung

Projekt: Vorantreiben Einrichtung Cyber Rapid Response Teams

Start: 21.2.2024
Ende: 1.1.2099
Nr.: 7153

Aktuelles Jahr
Status: grün
Fortschritt: 50 %

Zugrundeliegende Strategische Ziele

Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren

Gegenstand und Ziele

Basierend auf den Erfahrungen der ersten in Österreich ausgerufenen Cyberkrise im Jahr 2020 wurde die Notwendigkeit der Einrichtung von Cyber Rapid Response Teams erkannt. Sowohl die der Krise nachfolgenden Lessons Identified, als auch diverse Rechnungshofprüfungen attestierten den dringenden Bedarf.

Als das für den Aufbau und Bereitstellung am besten geeignete Ressort wurde das BMLV ausgemacht. Dieses kann sowohl präsente Kräfte als auch im Wege der Miliz Experten aus der Privatwirtschaft schnell verfügbar machen.

Beschreibung des Status

- 2020 Besprechungen auf Kabinettsebene zur Definition des Sollzustandes sowie Übernahme der Aufbauorganisation durch BMLV
- 2021 Ausplanung der Cyber Rapid Response Teams im Rahmen der Reorganisation des IKT- und Cybersicherheitszentrums (in weiterer Folge Dion 6). Anpassungen an den Orgplan wurden durch den Generalstab und KAB BMLV 06/23 genehmigt.
- Beginnen der Abstimmungen mit dem BMKÖS hinsichtlich strukturellem Aufbau

Mit Ende 2024 wurde im BMLV mit der Einrichtung der Cyber Rapid Response Teams begonnen.

Organisationsfeld

Bundeskanzleramt

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Cyberverteidigung

Projekt: Aufbau Nationale Cybersicherheits-zertifizierungsbehörde (NCZB)

Start: 1.3.2024
Ende: 31.12.2025
Nr.: 9174

Aktuelles Jahr
Status: grün
Fortschritt: 80 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

Einrichtung einer Zertifizierungsstelle nach dem EUCC für die Vertrauenswürdigkeitsstufe „hoch“ im BKA nach dem Rechtsakt zur Cybersicherheit (Verordnung 2019/881) bzw. Cybersicherheitszertifizierungs-Gesetz (BGBl. I Nr. 78/2024)

Freiwillige Zertifizierung von IKT-Produkten, -Diensten oder -Prozessen in den Stufen Niedrig (Selbstbewertung) – Mittel (Konformitätsbewertungsstelle) – Hoch (KBSt oder Behörde)

Notwendigkeit Schaffung einer Behörde zur Überwachung und Überprüfung der zertifizierten Produkte/Dienste/Prozesse

Beschreibung des Status

- Nationale Umsetzung der Verordnung mit Cybersicherheitszertifizierungs-Gesetz erfolgt
- Einrichtung der Zertifizierungsstelle im BKA erfolgt
- Personeller Aufwuchs gem. Gesetzes-WFA initiiert

Organisationsfeld

Bundeskanzleramt

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Internationale Zusammenarbeit

Projekt: Vorbereitung Umsetzung Cyber Resilience Act (CRA)

Start: 1.2.2025
Ende: 31.12.2027
Nr.: 9176

Aktuelles Jahr
Status: grün
Fortschritt: 5 %

Zugrundeliegende Strategische Ziele

- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Gegenstand und Ziele

(verpflichtende) Zertifizierung von Produkten mit digitalen Elementen welche in Europa produziert, vertrieben, eingeführt werden;

Produkte müssen nach grundlegenden Cybersicherheitsanforderungen konzipiert, entwickelt und hergestellt werden;

Produkte müssen ohne bekannter ausnutzbarer Schwachstellen und mit sicherer Standardkonfiguration auf dem Markt bereitgestellt werden in Kraft getreten mit 10.12.2024

Vollanwendung bis 11.12.2027

Zwischenschritt „Reporting für Schwachstellen“ bis 11.09.2026

Beschreibung des Status

- Teilnahme an den europäischen Verhandlungsgruppen
- Aufsetzen der Koordination der CRA relevanten Themen mit den gem. BMG zuständigen Organisationen

Organisationsfeld

Bundeskanzleramt

Herausforderungen

Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Kleine und mittlere Unternehmen (KMU)
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen

Projekt: Implementierung der CVD Plattform und Meldeprozesse gem. NIS2-RL

Start: 5.2.2025
Ende: 31.12.2025
Nr.: 9177

Aktuelles Jahr
Status: grün
Fortschritt: 15 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Gegenstand und Ziele

Gem. NIS2-RL sind die nationalen Rahmenbedingungen für die Schaffung eines Europäischen Schwachstellenregisters sicherzustellen.

Beschreibung des Status

- Dokument mit der Beschreibung des Prozesses wurde unter Federführung BMI und Einbindung der CSP entwickelt.
- Budgetäre Bedeckung für Entwicklung und Betrieb der Meldeplattform wurde vorgesehen
- Projekt zur Umsetzung in Konzeption

Organisationsfeld

Bundeskanzleramt

Herausforderungen

- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

- Vertrauen und Privatsphäre
- Cyberkriminalität und Strafverfolgung
- Internationale Zusammenarbeit

Projekt: Standardisierte/gemeinsame Ausbildung der CISOs in den Bundesministerien

Start: 31.5.2024
Ende: 31.5.2025
Nr.: 9178

Aktuelles Jahr
Status: grün
Fortschritt: 70 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen

Gegenstand und Ziele

Ziel ist es, nach der Etablierung der CISOs in den Bundesministerien, diese standardisiert gemeinsam auszubilden. Einerseits dient dies der Schaffung einer gemeinsamen Sprache und Verständnisses, als auch der Vernetzung über Ministeriengrenzen hinweg. Das BKA organisiert und führt zu diesem Zwecke eine allen Ministerien und obersten Organen zugänglichen Basiskurs für CISOs durch.

Beschreibung des Status

06/24 Konzeptionierung und Beauftragung Kurs

Q4/24 – Q2/25 Durchführung des CISO-Basiskurses im BKA

Teilnehmende Organisationen:
BHAG, Volksanwaltschaft, VFGH, Parlament, Hofburg, Rechnungshof, BRZ, BMKÖS, BVWG, BMK, BMAW, VWGH, BMEIA, BMLV, BMBWF, BMF, BMSGPK, BMI, BMJ, BML, BKA

Organisationsfeld

Bundeskanzleramt

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Widerstandsfähigkeit

Projekt: Förderung von Projekten zur Stärkung von Frauen und Mädchen im digitalen Raum

Start: 1.10.2023
Ende: 31.12.2025
Nr.: 9182

Aktuelles Jahr
Status: grün
Fortschritt: 60 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- In Österreich ist eine sichere Partizipation am gesellschaftlichen und politischen Leben im Cyberraum für Bürgerinnen und Bürger möglich

Gegenstand und Ziele

Im Rahmen des Förderaufrufes 2023 wurden € 1,079 Mio für „Maßnahmen zur Stärkung von Frauen und Mädchen in herausfordernden Zeiten mit Fokus auf Frauen in der Altersgruppe 60+ und unter Berücksichtigung ländlicher Regionen“ für Projekte (Laufzeit: 01.10.2023 bis 31.12.2024) in AT vergeben. Sechs der insgesamt 14 ausgewählten Projekte hatten den Schwerpunkt auf der Stärkung von Frauen und Mädchen im digitalen Raum. Der Förderaufruf 2024 stellt € 2 Mio für „Maßnahmen zur Stärkung von Frauen und Mädchen“ (Laufzeit: 01.09.2024 bis 31.12.2025) in AT zur Verfügung. Von den insgesamt 18 Projekten, legen sechs Projekte den Fokus auf die Stärkung von Frauen und Mädchen im digitalen Raum.

Im Rahmen der Projekte werden u. a. digitale Kompetenzen sowie Fähigkeiten und Kenntnissen zum Schutz vor Cybergewalt und Gefahren im Internet vermittelt.

Beschreibung des Status

Förderung von insgesamt 12 cybersicherheitsrelevanten Projekten:

1. frauenleben@digital.am.land
2. DigiFit60+: Weiterbildung von älteren Frauen zu Digitalbegleiterinnen
3. SELBSTsicherONLINE – Resilienzförderung im digitalen Raum
4. Gemeinsam gegen Cybergewalt
5. The future is Fem:AI*le: Das Projekt gegen digitale Ungleichheit
6. Digi-Held*innen
7. Sicher im Digitalen: Starke Mädchen, Starke Zukunft
8. Digital Navigator – From Passenger to Captain
9. Präventiv gegen digitale Gewalt!
10. 1#getreadywithme. Empowerment in Online-Kontexten für Mädchen* und junge Frauen* im ländlichen Raum
11. Angstfrei im Internet
12. cyber*power

Organisationsfeld

BKA III/2

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Bewusstseinsbildung (Awareness)
- Vertrauen und Privatsphäre
- Freier Meinungsbildungsprozess
- Bildung

Projekt: Umsetzung NIS 2 Richtlinie

Start: 16.1.2023
Ende: 31.10.2025
Nr.: 5120

Aktuelles Jahr
Status: gelb
Fortschritt: 80 %

Zugrundeliegende Strategische Ziele

- Österreich arbeitet in einem gesamtstaatlichen Ansatz stetig an der Weiterentwicklung seiner Rechtsgrundlagen zur Erhöhung der Cybersicherheit und Bekämpfung der Cyberkriminalität;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten
- 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
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

Am 16.01.2023 trat die NIS 2 Richtlinie in Kraft. Es handelt sich dabei um die Überarbeitung der NIS-Richtlinie aus dem 2016. Ziel ist es die Cybersicherheit der Europäischen Union und ihre Mitgliedstaaten weiter zu erhöhen und einen harmonisierten Sicherheitsstandard zu erreichen. Die Richtlinie war bis zum 17.10.2024 umzusetzen.

Beschreibung des Status

Erarbeitung der legistischen Entwürfe. Umsetzungsfrist 17.10.2024

BMI/BKA Arbeitsgruppen zur legistischen Aufbereitung eingesetzt.

Entwurf wurde erstellt und zur politischen Koordination vorgelegt. Einbindung der Länder bzw. Interessensvertretungen sowie Erstellung WFA erfolgt.

Vierwöchige Begutachtung im April abgeschlossen.

Eingebracht ins Plenum des Nationalrates; zugwiesen zum Ausschuss für innere Angelegenheiten.

Im BMI wurden mit dem Nationalen Cybersicherheitszentrum (NCSZ) die entsprechenden Strukturen geschaffen.

Im Nationalrat wurde der Gesetzesentwurf abgelehnt.

Im Dezember hat die EU ein Mahnverfahren gegen Österreich eingeleitet.

Replik wurde an die EK übermittelt, Aufschub wurde gewährt

Organisationsfeld

BKA I/8

Herausforderungen

- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Cyberkriminalität und Strafverfolgung
- Widerstandsfähigkeit
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Kleine und mittlere Unternehmen (KMU)
- Wirtschaftsstandort
- Forschung & Entwicklung

Projekt: Etablierung CISO in den Bundesministerien

Start: 15.12.2020
Ende: 31.12.2023
Nr.: 1005

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- 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
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen

Gegenstand und Ziele

Ein Chief Information Security Officer (CISO) ist im Ressort der Hauptansprechpartner in Fragen der Cybersicherheit. Er ist für die Wahrung des notwendigen und adäquaten Informationssicherheitsniveaus zuständig. Die Ressorts bekennen sich zur Etablierung eines CISOs im jeweiligen Bereich und stellen die Effektivität dieser Position durch geeignete Personalauswahl und Positionierung inner- halb der eigenen Entscheidungsstrukturen sicher.

Beschreibung des Status

- Dokument durch BKA erstellt
- Interministerielle Abstimmung eingeleitet (derzeit Veto von 1 Ministerium)
- Etablierung einer CISO Austauschrunde unter Einbindung aller Ministerien und obersten Organe

Organisationsfeld

BKA

Herausforderungen

Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

Widerstandsfähigkeit

Projekt: Sicherheitsstandards gem. NISG im öffentl. Sektor

Start: 15.12.2020
Ende: 31.12.2024
Nr.: 4

Aktuelles Jahr
Status: grün
Fortschritt: 90 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten

Gegenstand und Ziele

- Es sollen IT-Sicherheitsstandards in der Bundesverwaltung umgesetzt werden, die
  - gesetzlich verbindlich,
  - überprüfbar (auch durch externe Auditoren),
  - durchsetzbar sind.
- Umsetzung durch Anpassung des Netz-und Informationssystemsicherheitsgesetz (NIS-Gesetz), das die Richtlinie für Netz-und Informationssystemsicherheit (NIS-RL) umsetzt, im Bereich „Einrichtungen des Bundes“
- Beitrag zu einem gleichen Sicherheitsniveau zwischen Wirtschaft und Verwaltung

Beschreibung des Status

- Identifizierung der wesentlichen Dienste im BKA
- Erstellen Risikomatrix
- Aufnahme des Themas in Katalog Cybersicherheitsleitfaden (Empfehlungen der Generalsekretäre zur Erreichung eines hohen gemeinsamen Sicherheitsniveaus von Netz – und Informationssystemen)
- Umsetzung im Rahmen SFB und SFB2
- Veröffentlichung des Security Framework Bund interministeriell als auch im Wege der CSP

Organisationsfeld

BKA I/8

Herausforderungen

Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Widerstandsfähigkeit

Projekt: IT-Konsolidierungsprogramm: Security Framework Bund II – Anpassung an NIS 2

Start: 1.1.2024
Ende: 31.5.2025
Nr.: 7139

Aktuelles Jahr
Status: grün
Fortschritt: 30 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- 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
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

Projekt im Rahmen der IT-Konsolidierung

Basierend auf den Ergebnissen des Security Framework Bund Projektes, bei welchem 7 Ministerien mitgearbeitet haben und welches auf die Festlegung von Cyber-Mindestsicherheitsstandards im ministeriellen Bereich abzielte, wird mit dem Nachfolgeprojekt den neu hinzugekommen Anforderungen durch NIS 2 Rechnung getragen

Im Dezember 2024 wurde der Erstentwurf in der Runde der CISOs der Ministerien zirkuliert. Derzeit erfolgt die Einarbeitung der Rückmeldungen.

Beschreibung des Status

09/24 Vorprojektphase begonnen

11/24 Erstentwurf erstellt

12/24 Ministerien übergreifende Stellungnahmen einholen

01/25 Einarbeitung der Rückmeldungen

Organisationsfeld

BKA I/8

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Cyberverteidigung

Projekt: Erstellen eines Cyberübungsframeworks

Start: 22.11.2022
Ende: 31.3.2024
Nr.: 5123

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- In Österreich ist eine sichere Partizipation am gesellschaftlichen und politischen Leben im Cyberraum für Bürgerinnen und Bürger möglich
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- 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

Gegenstand und Ziele

Für Bundesministerien soll es möglich sein, anhand der Methoden-Leitfäden und Entscheidungsstrukturen des Cyberübungsframework, ihre Strategien auf strategische und operative Ziele umlegen können, um daraus Übungsziele für eine Cyberübung auswählen oder selbst formulieren zu können. Anhand dieser Übungsziele, kann ein Bundesministerium denjenigen Übungstyp ermitteln, der am besten geeignet ist um die Übungsziele zu erreichen bzw. beüben zu können, um in weiter Folge eine Cyberübung planen und durchführen zu können.

Beschreibung des Status

- Projekt Kick-Off November 2022
- Erfassen, Aufbereitung und Auswertung der nationalen und internationalen Grundlagendokumente bzw. Strategiepapiere, Nov. 2022–Jän. 2023
- Erarbeitung und Abstimmung der Grundkonzeption. Erarbeitung und Abstimmung von Methoden zur Identifikation „signifikant relevanter“ Übungsziele. Auflistung, Beschreibung und Nutzen bzw. Verwendungsmöglichkeit verschiedener Übungstypen für die Festlegung und Auswertung von Übungszielen, Jän. 2023–Feb. 2023
- Bearbeitung des Entscheidungsbaums und Aufbereitung der konzeptionellen Grundlagen
- Inhaltliche Bearbeitungen abgeschlossen
- Formatierung und Layoutierung
- Interne Qualitätssicherung
- Verteilung im ministeriellen Bereich

Organisationsfeld

BKA I/8

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

- Bildung
- Widerstandsfähigkeit

Projekt: Aufbau NCCA

Start: 15.12.2020
Ende: 31.12.2025
Nr.: 5

Aktuelles Jahr
Status: grün
Fortschritt: 90 %

Zugrundeliegende Strategische Ziele

– Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten
– Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen

Gegenstand und Ziele

- Schaffung Innerstaatlicher Voraussetzungen für die Teilnahme am europäischen Cybersicherheits-Zertifizierungsrahmen
- Umsetzung des EU Cybersecurity Acts (Verordnung (EU) 2019/881)
- Einrichtung einer Nationalen Behörde für die Cybersicherheitszertifizierung (National Cybersecurity Certification Authority – NCCA) im BKA durch Schaffung gesetzlicher Grundlagen
- Berücksichtigung bestehender Einrichtungen in der österreichischen IT-Sicherheitslandschaften durch Kooperationsformen

Beschreibung des Status

Optionen zur Implementierung ausgearbeitet

Entscheidung NCCA im BKA aufzubauen

Umsetzung durch Trennung operative und strategische Aufgaben

Konzeptionierung Aufbau und Ablauforganisation, Prozessdefinitionen

Gesetzesentwurf erstellt und in politische Koordination gegeben, WFA erstellt.

13.06.2024 im NR und am 27.06.2024 im BR angenommen.

Einrichtung erfolgt im BKA; warten auf erste EU-Schemata

Organisationsfeld

BKA I/8

Herausforderungen

Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

– Wirtschaftsstandort
– Widerstandsfähigkeit

Projekt: NCC-Förderung: Cyber Security Schecks

Start: 31.7.2023
Ende: 31.8.2025
Nr.: 7137

Aktuelles Jahr
Status: grün
Fortschritt: 90 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- 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
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen

Gegenstand und Ziele

KMU-Förderinitiative „Cyber Security Scheck 2023“ des Nationalen Koordinierungszentrums für Cybersicherheit: Mit der NIS2-Richtlinie gelten ab Oktober 2024 für viele Unternehmen verpflichtende Sicherheitsmaßnahmen und Meldepflichten im Bereich der Cybersicherheit. Ziel ist es, auf europäischer Ebene ein hohes Cybersicherheitsniveau sicherzustellen. Einen wichtigen Bestandteil dieser Strategie stellt die Stärkung der Resilienz und Reaktionsfähigkeit von Unternehmen gegenüber Cyberbedrohungen dar. Mit der Ausschreibung Cyber Security Scheck 2023, die über die FFG abgewickelt wird, werden österreichische KMU, die in den Anwendungsbereich der NIS2-Richtlinie fallen, bei der Vorbereitung zur Umsetzung der erforderlichen Sicherheitsmaßnahmen unterstützt. Die Finanzierung erfolgt zu gleichen Teilen über die EU und den Fonds Zukunft Österreich. Im Rahmen des geplanten Cyber Security Scheck 2024 ist vorgesehen, verbleibende Mittel für die Unterstützung von KMU, inkl. der NIS2-Lieferkette, bereitzustellen.

Beschreibung des Status

*Q1 bis Q3 2023: Entwicklung des Förderdesigns „Cyber Security Schecks“ durch die Österreichische Forschungsförderungsgesellschaft (FFG).

*Q4 2023: Veröffentlichung der Ausschreibung „Cyber Security Schecks 2023“ durch die FFG.

*Q2 und Q3 2024: Vorbereitung und Veröffentlichung der Ausschreibung „Cyber Security Schecks 2024“ durch die FFG.

*Q4 2023 bis Q3 2025: Laufende Implementierung und Abwicklung der „Cyber Security Schecks“ durch die FFG.

Organisationsfeld

NCC/FFG

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Kleine und mittlere Unternehmen (KMU)

Projekt: BKA – Förderungen von Projekten mit Schwerpunkt auf Bekämpfung von Cyber-Gewalt

Start: 1.11.2022
Ende: 31.12.2023
Nr.: 5124

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- In Österreich ist eine sichere Partizipation am gesellschaftlichen und politischen Leben im Cyberraum für Bürgerinnen und Bürger möglich

Gegenstand und Ziele

Förderaufruf „Maßnahmen zur Stärkung von Mädchen und Frauen in der digitalen Welt und Diversifizierung ihrer Ausbildungswege und Berufswahl mit Fokus auf MINT". Insgesamt werden Mittel in Höhe von 2 Millionen Euro für 17 Projekte in ganz Österreich vergeben. Sieben der ausgewählten Projekte haben ihren Schwerpunkt auf Cyber-Gewalt. Das Fördervolumen dieser sieben Projekte beträgt € 729.880,93. Ziele des Calls sind unter anderem die Stärkung von Mädchen und Frauen durch die Vermittlung von digitalen Kompetenzen, Schutz vor Gefahren im Internet, wie etwa Cybergrooming, Cyberstalking, Hass im Netz oder anderen Formen der Cyber-Gewalt sowie die Qualitätssicherung in der Beratung durch gezielte Fortbildungsmaßnahmen für die Beraterinnen der Frauen- und Mädchenberatungsstellen.

Beschreibung des Status

Förderung von 7 cybersicherheitsrelevanten Projekten.

13. Gendersensibel – Digital -Regional
14. Digi*Strong – Empowerment von Mädchen und jungen Frauen im digitalen Raum
15. worldwideweb.amazonen – Selbstverteidigung und Selbstwirksamkeit im digitalen Raum
16. Wissen und Struktur gegen Gewalt im Web
17. EmpowerHER*
18. Let IT Dance!
19. Digital Self: Persönliche Medienkompetenz und Resilienz

Organisationsfeld

BKA III/2

Herausforderungen

Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Bewusstseinsbildung (Awareness)
- Vertrauen und Privatsphäre

Projekt: Förderung von Fortbildungsseminaren zum Thema Cyber-Gewalt in (Ex-)Paarbeziehungen

Start: 1.4.2023
Ende: 31.3.2025
Nr.: 7130

Aktuelles Jahr
Status: grün
Fortschritt: 95 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- In Österreich ist eine sichere Partizipation am gesellschaftlichen und politischen Leben im Cyberraum für Bürgerinnen und Bürger möglich

Gegenstand und Ziele

Aufgrund der technischen Entwicklungen und fortschreitender Digitalisierung stellt Cybergewalt in (Ex-)Paarbeziehungen ein wachsendes Problem dar und äußert sich in unterschiedlichen Formen, wie Cybermobbing oder Stalking via GPS-Tracking. Die geförderten Fortbildungsseminare dienen der Vermittlung des spezifischen Wissens für die neuen Herausforderungen der Frauenberatungseinrichtungen und tragen damit zur Gewährleistung des notwendigen Know-hows und der entsprechenden Unterstützung bei.

Beschreibung des Status

Im Rahmen des Projekts sollen ab 01.04.2023 bis 31.03.2025 sechs zweitägige Schulungen abgehalten werden, wodurch zwischen 120 und 150 Mitarbeiterinnen und Mitarbeiter von Frauenberatungseinrichtungen aus allen Bundesländern geschult werden können.

Organisationsfeld

Bundeskanzleramt

Herausforderungen

Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Bewusstseinsbildung (Awareness)
- Vertrauen und Privatsphäre

Projekt: Ausbau des Zentralen Ausweichsystem des Bundes im Rahmen der Digitalen Arche

Start: 19.11.2021
Ende: 1.1.2025
Nr.: 1036

Aktuelles Jahr
Status: grün
Fortschritt: 45 %

Zugrundeliegende Strategische Ziele

Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen

Gegenstand und Ziele

Vision: Das gesamte digitale Gedächtnis Österreichs für die Ewigkeit erhalten

Mission: Den Gedächtnisinstitutionen und der Verwaltung soll die Möglichkeit gegeben werden, ihre Daten an einem krisensicheren Ort aufzubewahren und langfristig zu erhalten.

Beschreibung des Status

Aufbau eines POC im ZAS in St. Johann

Übernahme und Ausbau Rm 113/114

Bereitstellung 20 Racks 42HE

Abstimmungen mit BRZ für IaaS/PaaS Aufteilung nach ITIL am Laufen

Abstimmungen mit BMLV hinsichtlich kooperativem Aufbau/Betrieb

Projekt „Rechenzentrumservices“ mit BRZ durch BKA I/7 aufgesetzt

Konzeptionsprojekt mit BRZ aufgesetzt

Organisationsfeld

BKA I/8

Herausforderungen

Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Widerstandsfähigkeit

Projekt: Erhöhung der Cybersicherheit im BKA

Start: 2.11.2021
Ende: 31.12.2025
Nr.: 1029

Aktuelles Jahr
Status: grün
Fortschritt: 95 %

Zugrundeliegende Strategische Ziele

Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen

Gegenstand und Ziele

Ziel ist im ersten Schritt das Erstellen eines ISMS mit allen Kernprozessen inklusive 5 begleitenden Teilprojekten:

- Schaffen einer effektiven Bewältigung von Informationssicherheitsvorfällen
- Einführen eines Risikomanagements zur strukturierten Identifikation und Behandlung von Informationssicherheitsrisiken
- Umsetzen der Anforderungen für das BKA aus dem NISG
- Erarbeitung der Informationssicherheitstechnischen Voraussetzungen für die IT-Konsolidierung

Beschreibung des Status

Design des ISMS

Erhebung und Dokumentation des IST Status im BKA

Beschreibung aller Kernprozesse

Erstellung der Basisdokumente

Genehmigungsverfahren am Laufen

ISMS Operativ gestellt

Vorbereitungen für eine Zertifizierung nach ISO 27000

Organisationsfeld

BKA I/8

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Widerstandsfähigkeit

BMF

Projektverantwortliches Ressort
Bundesministerium für Finanzen

Stand: 5.3.2025

Nr.	Projekt	Status	Fortschritt	Start	Ende
1	1. Ausschreibung: Kybernet-Pass (K-PASS)	grün	100 %	30.10.2023	1.3.2024

Projekt: 1. Ausschreibung: Kybernet-Pass (K-PASS)

Start: 30.10.2023
Ende: 1.3.2024
Nr.: 9172

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit
- Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten

Gegenstand und Ziele

Kybernet-Pass (K-PASS) ist das erste eigenständige österreichische Cybersicherheitsforschungsprogramm, das den nationalen Bedarf und die Kompetenzen im Bereich Digitalisierung & Sicherheit mit den Cybersicherheitsinitiativen auf EU-Ebene eng verknüpft. Die Programmeigentümerschaft (Organisation und Finanzierung) von Kybernet-Pass liegt beim BMF, das Programm-Management (Projektbetreuung, Auszahlungen, Einreicherberatungen, etc.) bei der Österreichischen Forschungsförderungsgesellschaft FFG.

Durch die staatliche Beihilfe sollen marktnahe Forschungsergebnisse für Sicherheitsanwender (Bedarfsträger wie Polizei, Feuerwehr, Militär aber auch Betreiber Kritischer Infrastrukturen wie Telekombetreiber, Verbund oder Flughafen Wien) geschaffen werden, die durch die Entwicklung neuer Technologien und der Schaffung des erforderlichen Wissens die Sicherheit Österreichs erhöhen und Wertschöpfung generieren.

Beschreibung des Status

Abgeschlossen: 1. Ausschreibung von Kybernet-Pass mit Budget von € 5 Mio. hat am 30. Oktober 2023 begonnen und wurde am 01. März 2024 abgeschlossen. Insgesamt 10 Projekte wurden im Zuge der ersten Ausschreibung gefördert.

Organisationsfeld

BMF-VI/Stabsst.SiFo-TT

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Cyberverteidigung
- Internationale Zusammenarbeit
- Cyberkriminalität und Strafverfolgung
- Wirtschaftsstandort
- Kleine und mittlere Unternehmen (KMU)
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Forschung & Entwicklung
- Bildung

BMBWF

Projektverantwortliches Ressort
Bundesministerium für Bildung, Wissenschaft und Forschung

Stand: 5.3.2025

Nr.	Projekt	Status	Fortschritt / Projektampel	Start	Ende
1	Förderung der Cybersicherheit durch Pflichtfach Digitale Grundbildung	grün	100 %	1.10.2021	6.7.2022

Projekt: Förderung der Cybersicherheit durch Pflichtfach Digitale Grundbildung

Start: 1.10.2021
Ende: 6.7.2022
Nr.: 3097

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

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

Gegenstand und Ziele

Im Rahmen des Pflichtgegenstandes Digitale Grundbildung erwerben Schüler/innen auch Kompetenzen im Bereich Cybersicherheit. Diese sind im Lehrplan definiert und müssen von Lehrer/innen zwischen der 5. Schulstufe (1. Klasse Sek.1) und der 8. Schulstufe (4. Klasse Sek.1) verlässlich umgesetzt werden.

Beschreibung des Status

Gesetzlich umgesetzt. Start ist Schuljahr 2022/2023

Auszug aus dem Lehrplan angehängt.

Ist als laufendes Projekt zu verstehen – Enddatum entspricht der Veröffentlichung des Lehrplans. Wird inhaltlich weiterentwickelt.

Organisationsfeld

Praes-16

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Bildung
- Bewusstseinsbildung (Awareness)
- Freier Meinungsbildungsprozess
- Vertrauen und Privatsphäre
- Ethik

BMI

Projektverantwortliches Ressort
Bundesministerium für Inneres

Stand: 5.3.2025

Nr.	Projekt	Status	Fortschritt / Projektampel	Start	Ende
1	Ausbau des Computer Security Incident Response Teams des BMI (CSIRT-BMI)	grün	100 %	31.8.2020	2.5.2023
2	Betrieb von IKT-Lösungen zur frühzeitigen Erkennung von Risiken oder Vorfällen in NIS	grün	46 %	31.7.2022	29.9.2027
3	Ausbau C 4 zu moderner High Tech Einheit	grün	80 %	1.1.2021	30.6.2025
4	Umsetzung und/oder funktionelle Erweiterungen der IKT-Lösungen gem. NISG	grün	100 %	1.1.2021	30.9.2027
5	ÖSCS 2021	grün	100 %	16.8.2021	29.9.2023
6	Anpassung Cybercrime Delikte (Abstimmung mit BMJ)	grün	100 %	31.8.2021	1.9.2023
7	Cyber Cops-Bezirks IT Ermittler	grün	60 %	31.8.2021	30.9.2025
8	Betrieb einer Kollaborationsplattform für den IKDOK	grün	100 %	31.8.2022	29.6.2024
9	Erlassung von Geschäftsordnungen für die Koordinierungsstrukturen	grün	100 %	31.8.2022	29.12.2023
10	Erstellung von standardisierten Vorgehensweisen (SOPs) für die Koordinierungsstrukturen	grün	100 %	1.9.2022	31.3.2024
11	Erstmaßnahmen bei Cybersicherheitsvorfällen	grün	100 %	1.7.2022	31.12.2024
12	Schaffung einer IKT Lösung für besondere kriminalpolizeiliche Ermittlungen	grün	60 %	18.3.2021	31.12.2025

Projekt: Ausbau des Computer Security Incident Response Teams des BMI (CSIRT-BMI)

Start: 31.8.2020
Ende: 2.5.2023
Nr.: 1023

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren

Gegenstand und Ziele

Das CSIRT-BMI ist die zentrale Ansprechstelle des Innenressorts für interne IT-Security-Incidents nach dem Netz- und Informationssystemsicherheitsgesetz (NISG). Es sorgt durch präventive und reaktive Maßnahmen für eine Reduktion der IKT-Sicherheitsrisiken innerhalb des BMI sowie für eine rasche und kompetente Reaktion im Schadensfall. Die personellen und technischen Ressourcen sollen dazu ausgebaut werden.

Beschreibung des Status

Derzeit in Ausarbeitung

Organisationsfeld

BMI

Herausforderungen

Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

Widerstandsfähigkeit

Projekt: Betrieb von IKT-Lösungen zur frühzeitigen Erkennung von Risiken oder Vorfällen in NIS

Start: 31.7.2022
Ende: 29.9.2027
Nr.: 8162

Aktuelles Jahr
Status: grün
Fortschritt: 46 %

Beschreibung des Status

Vorbereitende Maßnahmen wurden eingeleitet; Status Quo noch nicht direkt verlassen

Zugrundeliegende Strategische Ziele

- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten
- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit

Organisationsfeld

BMI

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Wirtschaftsstandort
- Widerstandsfähigkeit

Gegenstand und Ziele

- Durch die Umsetzung u. a. eines sog IoC-Frühwarnsystems soll Einrichtungen im Rahmen des NISG idgF die freiwillige Teilnahme an IKT-Lösungen zur frühzeitigen Erkennung von Risiken und Vorfällen in Netz- und Informationssystemen ermöglicht werden.
- Für die Teilnahme gebührt dem Bund als Ersatz ein Pauschalbetrag, der nach Maßgabe der durchschnittlichen Kosten festgelegt wird.

Projekt: Ausbau C 4 zu moderner High Tech Einheit

Start: 1.1.2021
Ende: 30.6.2025
Nr.: 1024

Aktuelles Jahr
Status: grün
Fortschritt: 80 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Gegenstand und Ziele

Um den Herausforderungen im Bereich Cybercrime von Seiten des BMI auch in Zukunft gewachsen zu sein ist die Einrichtungen einer adäquaten Dienststelle unerlässlich. Das C4 soll diesen Ansprüchen angepasst werden und zu einer modernen Hightech-Crime-Abteilung ausgebaut werden. Der Ausbau umfasst insb: Umzug in ein adäquates Gebäude mit entsprechenden Räumlichkeiten/Anpassung personelle Ressourcen/Anpassung der bestehenden OE durch Einrichtung neuer Fachbereiche (Ermittlungen und IT-Forensik)

Beschreibung des Status

in Ausarbeitung

Datumsanpassung auf 30.06.2025 aufgrund verzögerter Neubewertung durch BMKOES und den damit verbundenen Funktionsbesetzungen

Organisationsfeld

BMI

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

Cyberkriminalität und Strafverfolgung

Projekt: Umsetzung und/oder funktionelle Erweiterungen der IKT-Lösungen gem. NISG

Start: 1.1.2021
Ende: 30.9.2027
Nr.: 1025

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;

Gegenstand und Ziele

Umsetzung und/oder funktionelle Erweiterungen der IKT-Lösungen gem. NISG insb NIS-Meldeanalysesystem (§ 11 NISG): Funktionelle Erweiterung der bestehenden Systematik und zur Verfügung stellen an die Partner im Rahmen IKDOK und OpKoord.

- IKDOK-Plattform (§ 12 NISG): Inbetriebnahme und zur Verfügung stellen IKDOK Plattform
- Betrieb von IKT-Lösungen zur Vorbeugung von Sicherheitsvorfällen (§ 13 NISG): Umsetzung des im NISG verankerten „IOC-basierten Frühwarnsystems“

Beschreibung des Status

in Ausarbeitung

Organisationsfeld

BMI

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Cyberkriminalität und Strafverfolgung

Projekt: ÖSCS 2021

Start: 16.8.2021
Ende: 29.9.2023
Nr.: 1026

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;

Gegenstand und Ziele

Die aktuellen Entwicklungen auf europäischer sowie auf sicherheitspolitischer Ebene machen es notwendig einen umfassenden Maßnahmenkatalog des BMI als Teil der ÖSCS 2021 auszuarbeiten. Zur Ausarbeitung dieses Maßnahmenkatalogs für das BMI ist ein Projekt im Programm zur Umsetzung des EU Cybersicherheitspakets 2020 im BMI eingerichtet.

Beschreibung des Status

in Ausarbeitung

Organisationsfeld

BMI

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Cyberkriminalität und Strafverfolgung

Projekt: Anpassung Cybercrime Delikte (Abstimmung mit BMJ)

Start: 31.8.2021
Ende: 1.9.2023
Nr.: 1027

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten
- Österreich arbeitet in einem gesamtstaatlichen Ansatz stetig an der Weiterentwicklung seiner Rechtsgrundlagen zur Erhöhung der Cybersicherheit und Bekämpfung der Cyberkriminalität;

Gegenstand und Ziele

Cybercrime ist der am stärksten wachsende Bereich im Kriminalitätsumfeld. Im Vergleich zu ähnlich gelagerten klassischen Delikten sind Cybercrime-Delikte im Strafausmaß wesentlich geringer bewertet. Eine Anhebung der Strafausmaße würde mehr Möglichkeiten für die Ermittlungsbehörden bedeuten, was wiederum zu einer höheren Aufklärungsrate und damit zu mehr Cybersicherheit beitragen würde. Die Abstimmung mit dem BMJ ist Voraussetzung für diese Maßnahme.

Beschreibung des Status

in Planung

Organisationsfeld

BMI

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

Cyberkriminalität und Strafverfolgung

Projekt: Cyber Cops-Bezirks IT Ermittler

Start: 31.8.2021
Ende: 30.9.2025
Nr.: 1028

Aktuelles Jahr
Status: grün
Fortschritt: 60 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten

Gegenstand und Ziele

Der Großteil der Anzeigen, auch im Cybercrime-Bereich, wird an Polizeiinspektionen in den Bezirken herangetragen. Es ist wichtig, dass dort gut ausgebildete Beamte Dienst versehen, welche professionelle Anzeigenaufnahmen machen können sowie wichtige erste Ermittlungsschritte setzen. Durch eine substanzielle Aufstockung der derzeit vorhandenen Bezirks IT-Ermittler (Cybercops) soll gewährleistet werden, dass es flächendeckend Cybercops gibt. Dies trägt zu einer höheren Aufklärungsrate und CyberSi.

Beschreibung des Status

n/a

Organisationsfeld

BMI

Herausforderungen

Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

Cyberkriminalität und Strafverfolgung

Projekt: Betrieb einer Kollaborationsplattform für den IKDOK

Start: 31.8.2022
Ende: 29.6.2024
Nr.: 3099

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- 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
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Gegenstand und Ziele

Durch das BMI wird den Teilnehmern des IKDOK eine Kollaborationsplattform zur Organisation und Wahrnehmung der Aufgaben gemäß § 7 Abs. 1 NISG zur Verfügung gestellt. Dazu wird eine IKDOK-Suite entwickelt und betrieben, um die Erstellung der Lagebilder zu unterstützen sowie eine gesicherte Kommunikation sicherzustellen.

Beschreibung des Status

Aktuell wird das Projekt evaluiert. Der Projektantrag wird in aktualisierter Form neu gestellt werden. Kernpunkte des Projekts sind: Entwicklung einer IKDOK-Suite mit: zentrales Login und Berechtigungsmanagement; Einbindung erforderlicher Applikationen (erweiterbar); Betrieb durch einen IKDOK-Teilnehmer.

Organisationsfeld

BMI

Herausforderungen

Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Bewusstseinsbildung (Awareness)
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen

Projekt: Erlassung von Geschäftsordnungen für die Koordinierungsstrukturen

Start: 31.8.2022
Ende: 29.12.2023
Nr.: 3100

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten
- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren

Gegenstand und Ziele

Für IKDOK und OpKoord sind gemäß Ermächtigung des NISG Geschäftsordnungen zu erstellen und zu erlassen. Dabei sind auch der Prozess zur Erstellung des Lagebildes festzulegen sowie eine einheitliche Anwendung einer abgestimmten Taxonomie zu empfehlen

Beschreibung des Status

Aktuell erfolgt die Überarbeitung vorhandener Entwürfe der Geschäftsordnungen als Grundlagen für weitere Abstimmung in den Koordinierungsstrukturen.

Organisationsfeld

BMI

Herausforderungen

Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Bewusstseinsbildung (Awareness)
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Widerstandsfähigkeit

Projekt: Erstellung von standardisierten Vorgehensweisen (SOPs) für die Koordinierungsstrukturen

Start: 1.9.2022
Ende: 31.3.2024
Nr.: 3101

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Beschreibung des Status

Aktuell erfolgt die Erstellung der SOPs parallel zum Entwurf der Geschäftsordnungen der Koordinierungsstrukturen.

Zugrundeliegende Strategische Ziele

- Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- 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
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren

Organisationsfeld

BMI

Herausforderungen

Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Bewusstseinsbildung (Awareness)
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen

Gegenstand und Ziele

Durch die Erstellung von standardisierten Vorgehensweisen (Standard Operating Procedure – SOP) ist die Zusammenarbeit innerhalb von IKDOK und OpKoord einheitlich und klar zu regeln. Die SOPs regeln unter anderem den Prozess zur Erstellung des Lagebildes, die anzuwendende Taxonomie oder die Vorgehensweisen in unterschiedlichen Eskalationsstufen im Detail.

Projekt: Erstmaßnahmen bei Cybersicherheitsvorfällen

Start: 1.7.2022
Ende: 31.12.2024
Nr.: 5121

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Beschreibung des Status

Im Plan (Anmerkung: Anpassung hinsichtlich Abgang ursprünglicher Ansprechpartner)

Zugrundeliegende Strategische Ziele

Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren

Organisationsfeld

BMI

Gegenstand und Ziele

Erstellung eines kompletten Ausbildungskonzepts für ein einwöchiges Seminar für Erstmaßnahmen bei IT- und Cybersicherheitsvorfällen im Zuständigkeitsbereich der LSEs und der DSN in Bezug zu den Fachbereichen der Digitalen Forensik, der Digitalen Ermittlungen, der Cyberprävention und vor allem der Cybersicherheit. Ziel ist es pro Bundesland drei Kolleginnen und Kollegen der LSEs für Erstmaßnahmen bei Cybersicherheitsvorfällen bis Ende 2024 fachlich zu schulen, zu vernetzen und einen aktiven Austausch zu Themen des Cyberkrisenmanagements zwischen den Teilnehmern zu etablieren.

Herausforderungen

Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

Widerstandsfähigkeit

Projekt: Schaffung einer IKT Lösung für besondere kriminalpolizeiliche Ermittlungen

Start: 18.3.2021
Ende: 31.12.2025
Nr.: 5122

Aktuelles Jahr
Status: grün
Fortschritt: 60 %

Zugrundeliegende Strategische Ziele

Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten

Gegenstand und Ziele

Durch die globale Vernetzung und stetig zunehmende Digitalisierung entstehen neue Möglichkeiten und modi operandi für die Begehung von neuen Deliktsformen. In fast allen Kriminalitätsbereichen haben sich klassische Begehungsformen in den digitalen Bereich verlagert. Insbesondere für die Fallbearbeitung im Kriminaldienst wird der Einsatz technischer Hilfsmittel unumgänglicher. Die Kriminalpolizei benötigt daher eine zeitgemäße, technische Möglichkeit, elektronische Beweismittel zu sichten, auszuwerten und darüber hinaus grundlegende Ermittlungen im Internet durchzuführen. Ziel des Projekts ist daher die Konzeption einer IKT Lösung für den kriminalpolizeilichen Dienst des BMI für besondere Ermittlungs- und Analysetätigkeiten.

Beschreibung des Status

im Plan

Organisationsfeld

BMI

Herausforderungen

Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

Cyberkriminalität und Strafverfolgung

BMJ

Projektverantwortliches Ressort
Bundesministerium für Justiz

Stand: 5.3.2025

Nr.	Projekt	Status	Fortschritt / Projektampel	Start	Ende
1	Einrichtung von Cybercrime Kompetenzstellen an Staats-anwaltschaften	grün	100 %	1.10.2022	29.6.2023

Projekt: Einrichtung von Cybercrime Kompetenzstellen an Staatsanwaltschaften

Start: 1.10.2022
Ende: 29.6.2023
Nr.: 3102

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich arbeitet in einem gesamtstaatlichen Ansatz stetig an der Weiterentwicklung seiner Rechtsgrundlagen zur Erhöhung der Cybersicherheit und Bekämpfung der Cyberkriminalität;
- Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten

Gegenstand und Ziele

Einrichtung von Cybercrime Kompetenzstellen an allen Staatsanwaltschaften sowie Ausstattung dieser mit zusätzlichen Planstellen. Ergänzend dazu wird der zentral im BMJ eingerichtete Pool an IT-Expert:innen auf 20 Personen erweitert und eine dedizierte Zuordnung von Ansprechpartnern je Oberstaatsanwaltschaft eingerichtet.

Beschreibung des Status

Cybercrime Kompetenzstellen bzw. Kontaktstellen wurden an den Staatsanwaltschaften eingerichtet. Personalsuche für Cybercrime-Staatsanwält:innen und IT-Expert:innen im Laufen.

Organisationsfeld

BMJ

Herausforderungen

Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

Cyberkriminalität und Strafverfolgung

BMLV

Projektverantwortliches Ressort
Bundesministerium für Landesverteidigung

Stand: 5.3.2025

Nr.	Projekt	Status	Fortschritt / Projektampel	Start	Ende
1	Ausbau und verstärkte EU-Koordinierung nationaler milCERTs (Beitrag zum CDPF-Review der EU)	rot	40 %	9.9.2021	31.12.2026
2	Erstellung eines Querschnittskonzepts „Einsatz im Cyber-Raum“	grün	100 %	3.7.2022	31.12.2023
3	Umsetzung der EU Cyber Defence Policy	grün	25 %	10.7.2023	31.12.2028
4	Erstellung eines umfassenden militärischen Cyber-Lagebildes	gelb	15 %	1.1.2024	31.12.2028
5	Aufbau einer militärischen Cyber Range	rot	15 %	31.3.2021	31.12.2024
6	Aufbau von Cyber Rapid Response Teams (CRRT) im BMLV	rot	40 %	31.3.2024	31.12.2024
7	Bereitstellung einer KI Risikoanalyse für einsatzrelevante IKT Systeme des ÖBH	grün	10 %	1.12.2024	31.12.2025
8	Gezielte Förderung von Innovation im Cyber-Raum durch konkrete Maßnahmen	grün	10 %	30.6.2024	31.12.2026
9	Intensivierung der internationalen Kooperation zur besseren Beitragsleistung bei Cyber-Vorfällen	grün	60 %	20.3.2013	1.1.2026
10	Nutzung von Cyber-Threat-Intel-Plattformen zur Verdichtung des Cyber-Lagebildes	rot	90 %	2.1.2022	31.12.2027
11	Ausbau von Fähigkeiten zur Erkennung gezielter Manipulation des Informationsraums	grün	55 %	1.1.2021	31.12.2031
12	Ausbau von Fähigkeiten zur Netzwerkforensik- und Malwareanalyse sowie Reverse-Engineering	rot	70 %	1.1.2021	31.12.2023
13	Beitrag zum gesamtstaatlichen Lagebild über den Weg des IKDOK	grün	100 %	20.3.2013	1.1.2030
14	Erstellung einer Cyberverteidigungsstrategie und Fähigkeitenprofils zur Cyberverteidigung	grün	100 %	1.2.2021	31.12.2023
15	Stärkung der Cybersicherheit durch Schutz der eigenen IKT-Systeme	rot	40 %	12.10.2020	31.12.2026
16	Fokus auf technische Entwicklungen (Digitalisierung) in der Streitkräfteplanung und -entwicklung	grün	40 %	26.9.2017	26.9.2032
17	Verankerung der Cyber-Domäne im MSK und Aufbau von Cyber-Kräften im ÖBH	grün	60 %	25.9.2017	26.9.2032
18	Bereitstellung von OpenSource-Information durch das CyDok&ForschZ (Recherche und Analyse)	grün	100 %	1.1.2014	31.12.2024
19	Einführung des FH-Bachelorstudiengangs „Militärische IKT-Führung“ an der TherMilAk	grün	100 %	31.8.2022	31.12.2023
20	Neugestaltung der ADV-Sonderverträge für IT-Personal (FF BMKÖS)	grün	80 %	1.1.2021	31.12.2026

Projekt: Ausbau und verstärkte EU-Koordinierung nationaler milCERTs (Beitrag zum CDPF-Review der EU)

Start: 9.9.2021
Ende: 31.12.2026
Nr.: 1018

Aktuelles Jahr
Status: rot
Fortschritt: 40 %

Zugrundeliegende Strategische Ziele

- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen

Gegenstand und Ziele

Das Cyberdefence Policy Framework (CDPF) konkretisiert die (militärische) Ambition sowie Fähigkeitenentwicklung der EU und MS für die nächsten 5-10 Jahre.

Mit September 2021 begann ein Review-Prozess des CDPF, der bis Mitte 2022 andauern wird.

Ziel: Eintreten für Kapazitätenausbau und stärkere Koordinierung der nationalen milCERTs auf EU-Ebene (mittelfristig) sowie für die Etablierung eines gemeinsamen EU-milCERT (langfristig) im Rahmen des CDPF-Review-Prozesses. Diese Maßnahme wird voraussichtlich aufgrund der neuen EU Cyber Defence Policy (Mai 2023) angepasst werden.

Beschreibung des Status

- Zurzeit kein weiterer Ausbau
- Im Rahmen des 1. CDPF-Review-Workshops des EAD am 10.09.21 erfolgte eine Ankündigung sowie im Anschluss eine schriftliche Übermittlung des AUT-Vorschlags
- Bis Okt 2022 im Plan, danach Verzögerungen wegen fehlender Umsetzung der Orgplan-Erweiterungen. Personalressourcen zur Zuarbeit im Projekt und dem gestartetem milCERT-Info-Sharing auf EU-Ebene können nicht beigestellt werden und wirken sich negativ auf die österreichische Verteidigungsfähigkeit aus.

Bisherige Aktivitäten konnten nur durch Ressourcen-Abzug aus anderen Projekten temporär wahrgenommen werden. Die AUT Mitarbeit wurde 2024 durch aktive Teilnahme an MIC und MICNET zur Erprobung und Verbesserung des Informationsaustauschs zwischen EU MilCERTs fortgeführt.

Organisationsfeld

BMLV

Herausforderungen

Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Cyberverteidigung
- Internationale Zusammenarbeit

Projekt: Erstellung eines Querschnittskonzepts „Einsatz im Cyber-Raum“

Start: 3.7.2022
Ende: 31.12.2023
Nr.: 7128

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Beschreibung des Status

Das Querschnittskonzept wurde im Oktober 2023 verfügt. Projekt erfolgreich abgeschlossen.

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen

Organisationsfeld

BMLV

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Cyberverteidigung
- Internationale Zusammenarbeit

Gegenstand und Ziele

Durch die Erstellung des Querschnittskonzepts „Einsatz im Cyber-Raum“ werden Grundlagen zur (Weiter-)Entwicklung der Waffengattungen der Cyber-Kräfte weiter detailliert.

Projekt: Umsetzung der EU Cyber Defence Policy

Start: 10.7.2023
Ende: 31.12.2028
Nr.: 7129

Aktuelles Jahr
Status: grün
Fortschritt: 25 %

Zugrundeliegende Strategische Ziele

- Österreich arbeitet in einem gesamtstaatlichen Ansatz stetig an der Weiterentwicklung seiner Rechtsgrundlagen zur Erhöhung der Cybersicherheit und Bekämpfung der Cyberkriminalität;
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

Ressortinterne Umsetzung der festgelegten 46 Maßnahmen des EU-Umsetzungsplans zur Cyber Defence Policy (Juli 2023). BMLV-spezifische Maßnahmen müssen identifiziert und in den Zuständigen Dienststellen umgesetzt werden.

Beschreibung des Status

Im Frühjahr 2024 wurde der erste Fortschrittsbericht auf EU-Ebene veröffentlicht und im Herbst 2024 wurde der zweite BMLV-interne und gesamtstaatliche Stand erneut erhoben. Umsetzung auf EU-Ebene schreitet planmäßig voran, hängt jedoch BMLV-intern von der OrgPlan Umsetzung ab.

Organisationsfeld

BMLV

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

- Internationale Zusammenarbeit
- Cyberverteidigung
- Cyberkriminalität und Strafverfolgung
- Widerstandsfähigkeit

Projekt: Erstellung eines umfassenden militärischen Cyber-Lagebildes

Start: 1.1.2024
Ende: 31.12.2028
Nr.: 8167

Aktuelles Jahr
Status: 🟡 gelb
Fortschritt: 15 %

Zugrundeliegende Strategische Ziele

- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit

Gegenstand und Ziele

Schaffung eines umfassenden Cyber-Lagebildes, in dem Erkenntnisse der operativen Ebene mit jenen der strategischen Ebene verschmolzen und zu einer effizienteren Erkenntnisgewinnung genutzt werden. Ziel ist es ein ganzheitliches Situationsbewusstsein im Cyber- und Informationsbereich für das gesamte Österreichische Bundesheer zu entwickeln. Dies verfolgt einen koordinierten und integrierten Ansatz zur Cyber-Sicherheit auf allen Ebenen der Organisation.

Beschreibung des Status

Informationsbedarf nach wie vor offen, u. a. aufgrund fehlender Vorgaben durch fehlende Ressourcen. Es wird daran gearbeitet, insbes. auch im Hinblick auf die künftige IKT-Infrastruktur „ÖBH2032+“.

Organisationsfeld

BMLV/Direktion IKT & Cyber

Herausforderungen

Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Cyberverteidigung

Projekt: Aufbau einer militärischen Cyber Range

Start: 31.3.2021
Ende: 31.12.2024
Nr.: 8168

Aktuelles Jahr
Status: 🔴 rot
Fortschritt: 15 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- 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
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

Ziel ist die Schaffung einer virtuellen Umgebung, innerhalb derer sowohl Cyber-Angriff und Cyber-Verteidigung geübt, als auch neue Technologien erprobt werden können, ohne produktive Systeme zu gefährden. Diese Plattformen bieten realistische Simulationen von Ereignissen im Cyber-Raum und ermöglichen es so, reale Einsatzsituationen zu simulieren. Der Fokus liegt dabei auf der Entwicklung von Abwehrstrategien, der Erkennung von Angriffen und der Verbesserung technischer und personeller Fähigkeiten.

Beschreibung des Status

Operationalisierung verzögert sich weiterhin. Beschaffungen der nötigen Ausrüstung sind verzögert, aber in Bearbeitung. Da die Maßnahme bereits stark verzögert ist und das Umsetzungsziel verfehlt, wäre für eine Umsetzung in absehbarer Zeit eine unmittelbare Priorisierung auf allen Ebenen notwendig. Allen voran betrifft dies die zeitnahe Verfügung eines OrgPlans für den Ausbau eines operativen Teams (aktuell systemisiert sind 20 % der erforderlichen und ausgeplanten Positionen).

Organisationsfeld

BMLV/Direktion IKT & Cyber

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Forschung & Entwicklung
- Widerstandsfähigkeit
- Cyberverteidigung
- Internationale Zusammenarbeit

Projekt: Aufbau von Cyber Rapid Response Teams (CRRT) im BMLV

Start: 31.3.2024
Ende: 31.12.2024
Nr.: 8169

Aktuelles Jahr
Status: 🔴 rot
Fortschritt: 40 %

Beschreibung des Status

Beschaffungen der nötigen Ausrüstung sind aufgrund OrgPlan verzögert, aber in Bearbeitung.

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- 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
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Organisationsfeld

BMLV/Direktion IKT & Cyber

Herausforderungen

Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Cyberverteidigung
- Internationale Zusammenarbeit

Gegenstand und Ziele

Aufgrund der wachsenden Bedrohung im Cyber-Raum und der steigenden Zahl kritischer Cyber-Sicherheitsvorfälle ist die Einrichtung eines CRRT für das Österreichische Bundesheer zum Schutz der eigenen IKT-Systeme und im Falle eines Vorfalls auf nationaler und EU-Ebene eine unabdingbare Voraussetzung geworden. Der Aufbau der nationalen Fähigkeit ist daher dringend erforderlich und muss zeitnah umgesetzt werden.

Projekt: Bereitstellung einer KI Risikoanalyse für einsatzrelevante IKT Systeme des ÖBH

Start: 1.12.2024
Ende: 31.12.2025
Nr.: 8170

Aktuelles Jahr
Status: grün
Fortschritt: 10 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen

Gegenstand und Ziele

Es geht darum, potenzielle Risiken zu evaluieren, die sich für das Österreichische Bundesheer aus dem Einsatz von künstlicher Intelligenz (KI) durch staatliche und nichtstaatliche Akteure ergeben. Zentral ist die Frage, welche Risiken für welche IKT-Systeme durch den Aufstieg und den vermehrten Einsatz von KI zu erwarten sind.

Beschreibung des Status

Start geplant für Q1 2025

Organisationsfeld

BMLV/Direktion IKT & Cyber

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Forschung & Entwicklung
- Widerstandsfähigkeit
- Cyberverteidigung

Projekt: Gezielte Förderung von Innovation im Cyber-Raum durch konkrete Maßnahmen

Start: 30.6.2024
Ende: 31.12.2026
Nr.: 8171

Aktuelles Jahr
Status: grün
Fortschritt: 10 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- 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
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit

Gegenstand und Ziele

Durch die Einführung bzw. Bereitstellung gezielter Maßnahmen zur Förderung von Innovation soll die Fähigkeiten des ÖBH im Cyber-Raum insgesamt gestärkt werden. Zudem werden somit Impulse gesetzt, um sich den ständig wandelnden Cyber-Bedrohungen anzupassen und innovative Lösungen zur Stärkung der nationalen Cyber-Sicherheit und- Verteidigung zu entwickeln.

Beschreibung des Status

Als Teil dieses Innovationspakets hat das MilCyZ als erste Maßnahme eine neue Veranstaltungsreihe ins Leben gerufen, um Experten aus Wissenschaft, Wirtschaft und Verwaltung zu den neuesten Themen im Bereich Sicherheit und Verteidigung an einen Tisch zu bringen. „InnoVision“ hat als zukunftsorientierte Veranstaltungsreihe das Ziel, einen Raum zu schaffen, in dem Wissen geteilt, Ideen geboren und bahnbrechende Technologien vorangetrieben werden. Das erste Event fand am 15.11.2024 statt.

Weitere Maßnahmen zur Innovationsstärkung, inklusive mehrerer Experten-Fokusgruppen werden 2025 abgehalten.

Organisationsfeld

BMLV/Direktion IKT & Cyber

Herausforderungen

Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Forschung & Entwicklung
- Cyberverteidigung

Projekt: Intensivierung der internationalen Kooperation zur besseren Beitragsleistung bei Cyber-Vorfällen

Start: 20.3.2013
Ende: 1.1.2026
Nr.: 1050

Aktuelles Jahr
Status: grün
Fortschritt: 60 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen

Gegenstand und Ziele

Durch internationale Kooperation und Informationsaustausch erhöht das BMLV seine INTEL-Fähigkeiten und bringt diese auch ins gesamtstaatliche Cyber-Lagebild ein.

Ziel ist die Verbesserung der gesamtstaatlichen Beitragsleistung bei Erkennung, Abwehr und Zuordnung von Cyber-Vorfällen.

Beschreibung des Status

- Die Umsetzung der EU Cyber Defence Policy auf EU- und nationaler Ebene wird Österreichs Fähigkeiten und Beitragsleistung zur Cyber-Verteidigung der EU und nationalen Resilienz weiter stärken
- Die Nutzung von Austauschplattformen (z. B. DACH, EU, NATO PfP) wird intensiviert, jedoch können diese aufgrund mangelnder Personalressourcen derzeit nur unzureichend genutzt werden.

Organisationsfeld

BMLV

Herausforderungen

Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Internationale Zusammenarbeit
- Cyberverteidigung

Projekt: Nutzung von Cyber-Threat-Intel-Plattformen zur Verdichtung des Cyber-Lagebildes

Start: 2.1.2022
Ende: 31.12.2027
Nr.: 1051

Aktuelles Jahr
Status: rot
Fortschritt: 90 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;

Gegenstand und Ziele

Durch den Betrieb von Cyber-Threat-Intel-Plattformen kann das Cyber-Lagebild deutlich dichter und besser unterfüttert werden. Dadurch kann bei einem Cyberangriff zumindest die politisch geographische Zuordnung besser und schneller erfolgen.

Ziel ist die Verbesserung der evidenzbasierten Unterstützungsleistung zum politischen Attribuierungsprozess.

Beschreibung des Status

Cyber-Threat-Intel-Plattformen sind up and running und werden aktiv im BMLV betrieben. Implementierung in alle relevante Analyse-Prozesse läuft.

Die Analyse-Fähigkeit und hier insbesondere die abschließende Implementierung und Verknüpfung in die bestehende Landschaft sind aufgrund fehlender Personal-Kapazitäten stark eingeschränkt. Die zeitgemäße Umsetzung der erforderlichen Integrationen ist gefährdet.

Organisationsfeld

BMLV

Herausforderungen

Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

Cyberverteidigung

Projekt: Ausbau von Fähigkeiten zur Erkennung gezielter Manipulation des Informationsraums

Start: 1.1.2021
Ende: 31.12.2031
Nr.: 1052

Aktuelles Jahr
Status: grün
Fortschritt: 55 %

Beschreibung des Status

Konzepte zu InfoOps und StratKomm gehen derzeit in die Realisierung.

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen

Gegenstand und Ziele

Angesichts der stetigen Zunahme hybrider Bedrohungen, inkl. Desinformation, muss das BMLV seine eigenen Fähigkeiten zur Erkennung gezielter Manipulation des Informationsraums ausbauen, um eine sicherheitspolitische Vorteilnahme (sowohl staatlich als auch nichtstaatlich) ausländischer Akteure zu Verhindern.

Ziel ist der langfristige Schutz des Informationsumfeldes Österreichs gegen Beeinflussung durch äußere Akteure.

Organisationsfeld

BMLV

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Bewusstseinsbildung (Awareness)
- Cyberverteidigung

Projekt: Ausbau von Fähigkeiten zur Netzwerkforensik- und Malwareanalyse sowie Reverse-Engineering

Start: 1.1.2021
Ende: 31.12.2023
Nr.: 1053

Aktuelles Jahr
Status: rot
Fortschritt: 70 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Gegenstand und Ziele

Die Behandlung und Abwehr von Cyber-Vorfällen erfordern insbesondere den Ausbau von technischen (Geräte) sowie personellen (Ausbildung) Fähigkeiten. Dazu gehören die Bereiche Netzwerkforensik- und Malwareanalyse sowie Reverse-Engineering. Ziel ist es, Cyber-Vorfälle schnell und effektiv erkennen und abwehren zu können.

Beschreibung des Status

Netzwerk und Computerforensik sind eingeführte Technologien. Der Bereich des Reverse Engineerings ist verbesserungswürdig, aber auch bereits funktionell.

Aufgrund der fehlenden OrgPlan Bearbeitung fand kein weiterer Fähigkeitenaufbau seit 2021 statt.

Organisationsfeld

BMLV

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Cyberverteidigung
- Widerstandsfähigkeit

Projekt: Beitrag zum gesamtstaatlichen Lagebild über den Weg des IKDOK

Start: 20.3.2013
Ende: 1.1.2030
Nr.: 1039

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;

Gegenstand und Ziele

Im Wege des IKDOK werden gesamtstaatlich relevante Informationen zur Akteuren und deren potentiell wirksam werdenden Cyber-Bedrohungen mit den IKDOK-Teilnehmern getauscht und in das regelmäßig verteilte IKDOK-Lagebild aufgenommen.

Ziel ist es das gesamtstaatliche Cyber-Lagebild zu verbessern und damit potenzielle Cyber-Bedrohungen früh zu erkennen bzw. antizipieren.

Beschreibung des Status

MilCyZ ist bereits langjähriges Mitglied und beteiligt sich aktiv an der Gestaltung zum wöchentlichen Lagebild, als auch bei Sonderlagebildern des IKDOK.

Organisationsfeld

BMLV

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Bewusstseinsbildung (Awareness)
- Cyberverteidigung

Projekt: Erstellung einer Cyberverteidigungsstrategie und Fähigkeitenprofils zur Cyberverteidigung

Start: 1.2.2021
Ende: 31.12.2023
Nr.: 1042

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen
- Österreich arbeitet in einem gesamtstaatlichen Ansatz stetig an der Weiterentwicklung seiner Rechtsgrundlagen zur Erhöhung der Cybersicherheit und Bekämpfung der Cyberkriminalität;

Gegenstand und Ziele

Durch die Erstellung einer Cyberverteidigungsstrategie soll die strategische Ausrichtung der Cyberverteidigung im BMLV/ÖBH definiert werden. Die Strategie beruht auf den geltenden Rechtsgrundlagen, einer Bedrohungsanalyse und militärstrategischen Rahmenbedingungen bzw. Kooperationen der nationalen sowie internationalen Cyber-Sicherheit.

Ziel ist es, strategische Leitlinien und ein abgeleitetes Fähigkeitenprofil für das BMLV/ÖBH zur Cyberverteidigung zu entwickeln.

Beschreibung des Status

Die Richtlinie Cyberverteidigung wurde mit September 2023 verfügt und stellt die die Cyber-Strategie der Direktion IKT&Cyber dar. Diese wird zurzeit umgesetzt.

Organisationsfeld

BMLV

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Cyberverteidigung
- Widerstandsfähigkeit
- Internationale Zusammenarbeit

Projekt: Stärkung der Cybersicherheit durch Schutz der eigenen IKT-Systeme

Start: 12.10.2020
Ende: 31.12.2026
Nr.: 1043

Aktuelles Jahr
Status: rot
Fortschritt: 40 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- 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
- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren

Gegenstand und Ziele

Das BMLV/ÖBH ist bestrebt, die eigene Cybersicherheit durch Fördern des Bewusstseins sowie Etablierung von Schutzmaßnahmen der eigenen IKT-Systeme zu erhöhen.

Ziel ist die Entwicklung von Implementierungsschritten zur Verbesserung der lageangepassten Aufbereitung von Bedrohungen aus dem Cyber-Raum, Verteidigung militärischer Netze, Abwehr von Cyber-Angriffen und Ausbildung von Cyber-Kräften, unterstützt durch Sonderfinanzierungen.

Beschreibung des Status

Die ausstehenden, massiven zusätzlichen Personal- und Ressourcen-Aufwände werden seit nunmehr ~3 Jahren aufgrund der ReOrg nicht mehr bearbeitet, Hierdurch kann die Resilienz der Systeme nicht gemäß ihres Schutzbedarfes erfüllt werden. Der Ausblick ist hier klar negativ und fähigkeitsreduzierend, da die aktuelle Auftragslage mit der Personalsituation nicht bewältigbar ist und der steigenden Angriffe (quantitativ und qualitativ) mit der Reduktion der Verteidigungsfähigkeit einhergeht. Dementsprechend befindet sich diese Maßnahme derzeit im Stillstand. Wiederaufnahme ist soweit mit Abschluss ReOrg 2025 erhofft.

Organisationsfeld

BMLV

Herausforderungen

- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Cyberverteidigung

Projekt: Fokus auf technische Entwicklungen (Digitalisierung) in der Streitkräfteplanung und -entwicklung

Start: 26.9.2017
Ende: 26.9.2032
Nr.: 1045

Aktuelles Jahr
Status: grün
Fortschritt: 40 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen

Gegenstand und Ziele

Auf Basis der mil.strat. Grundlagendokumente, Planungszielen und -konzepten, wird die Ausrichtung des ÖBH mittel- bis langfristig auf neue Bedrohungen, inkl. erwartbare technologischen Entwicklungen, angepasst. Dies betrifft insb. die Cyber-Kräfte sowie die gesamte Digitalisierung der Streitkräfte.

Ziel ist der Schutz der IKT-Systeme des ÖBH bei Angriffen sowie bei Bedarf der verfassungsmäßigen Einrichtungen oder kritischer Infrastrukturen; Befähigung zum Kampf in Computernetzwerken im vollen Spektrum

Beschreibung des Status

- Aktueller Zeithorizont der Fähigkeiten- und Streitkräfteentwicklungsplanung ist 2032
- Stand Feb. 2025: Derzeit in planmäßiger Umsetzung

Organisationsfeld

BMLV

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

- Internationale Zusammenarbeit
- Cyberverteidigung

Projekt: Verankerung der Cyber-Domäne im MSK und Aufbau von Cyber-Kräften im ÖBH

Start: 25.9.2017
Ende: 26.9.2032
Nr.: 1044

Aktuelles Jahr
Status: grün
Fortschritt: 60 %

Zugrundeliegende Strategische Ziele

- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;

Gegenstand und Ziele

Im MSK 2017 wurden der Cyber-Raum als eigene Domäne definiert und die Cyber-Kräfte als Teilstreitkraft des ÖBH etabliert. Die Teilstreitkraft setzt sich aus Cyber-, IKT- und EloKa-Truppe (Elektronische Kampfführung) zusammen. Diese sind zuständig für den Einsatz im Cyber-Raum im Rahmen der militärischen LV, Beitragsleitung zur inneren Sicherheit und Auslandseinsätzen.

Ziel ist die Schaffung einer Grundlage für den Aufbau bzw. die laufende Fähigkeitenentwicklung von Cyber-Kräften im ÖBH.

Beschreibung des Status

Die Überarbeitung des MSK ist für 2025 avisiert.

Organisationsfeld

BMLV

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

- Internationale Zusammenarbeit
- Cyberverteidigung

Projekt: Bereitstellung von OpenSource-Information durch das CyDok&ForschZ (Recherche und Analyse)

Start: 1.1.2014
Ende: 31.12.2024
Nr.: 1040

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren

Gegenstand und Ziele

Das Cyberdokumentations- & Forschungszentrum der LVAk stellt täglich aktualisierte Fachinformationen nach verschiedensten Kategorien („Cyber“, „Kritische Infrastruktur“, uvm.) auf einer OSInfo-Plattform und Datenbank bereit. Die Recherche- und Analysedienste können bei Bedarf öffentl. Dienststellen jederzeit abgerufen und weiterverarbeitet werden, z. B. in Form eines Expert Horizon Scanning.

Ziel ist die Verbesserung des Cyber-Lagebildes, samt Folgenabschätzung, durch OSInfo-Recherche und -analyse.

Beschreibung des Status

- OSInfo-Plattform und Datenbank bereits seit 2014 operativ. Informationen und Analysen sind nach kurzer inhaltlicher und technischer Abstimmung jederzeit abrufbar bzw. auf Dauer aktivierbar
- Laufende Informations- und Analyseübermittlung an DSt des BMLV
- Noch keine direkte Schnittstelle in anderen Ministerien, Beiträge wären „on demand“ jederzeit abruf- bzw. aktivierbar
- Laufende Anpassungen und Ausbau der Systeme je nach Bedarf und Anforderung

Organisationsfeld

BMLV

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Forschung & Entwicklung
- Cyberverteidigung

Projekt: Einführung des FH-Bachelorstudiengangs „Militärische IKT-Führung“ an der TherMilAk

Start: 31.8.2022
Ende: 31.12.2023
Nr.: 1046

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

Das BMLV entwickelte infolge einer aus dem Bedrohungsbild abgeleiteten Empfehlung („Handlungsbedarf“ im „Cyberraum“ und „Informationsumfeld“) das Konzept einer alternativen Offiziersausbildung mit dem FH-Bachelorstudiengang „Militärische IKT-Führung“ an der Theresianischen Militärakademie ab 2022/23.

Ziel ist die Ausbildung ausreichend vieler IKT-Fachkräfte für den künftigen Bedarf im (militärischen) Cyber-Bereich.

Beschreibung des Status

Der Bachelor Studiengang MilIKTFü wird seit dem Wintersemester 2022/2023 an der Fachhochschule für angewandte Militärwissenschaften (Erhalter: Bund, FBM als oberste Erhaltervertreterin) durchgeführt. Maßnahme daher zu 100 % erfüllt.

Organisationsfeld

BMLV

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Cyberverteidigung
- Bildung

Projekt: Neugestaltung der ADV-Sonderverträge für IT-Personal (FF BMKÖS)

Start: 1.1.2021
Ende: 31.12.2026
Nr.: 1047

Aktuelles Jahr
Status: grün
Fortschritt: 80 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

BMLV ist Teil einer gesamtstaatlichen AG unter Federführung des BMKÖS. Die AG arbeitet an der Neugestaltung von ADV-Sonderverträgen für den gesamten Bundesbereich (aktuelle Richtlinie aus den 1990er Jahren).

Ziel ist die Anpassung der Richtverwendungen sowie der Entgeltansätze an aktuelle Erfordernisse angesichts des massiven Fortschritts im IT-Bereich. Dadurch soll der Bund attraktiver für IT-Personal gemacht werden. Dies könnte auch die personellen Ressourcen im Cyberbereich erhöhen.

Beschreibung des Status

Strukturumstellung gemäß Richtverwendung IT (RIVIT) wurde abgeschlossen und eine große Anzahl von ADV/SV-Bedienstete ins RIVIT-Vertragsschema gebracht. Sonderfälle sind weiterhin vorhanden.

Die Umsetzung befindet sich mit Stand Anfang 2025 in der Finalisierung.

Organisationsfeld

BMLV

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Cyberverteidigung

BMEIA

Projektverantwortliches Ressort

Bundesministerium für europäische und internationale Angelegenheiten

Stand: 5.3.2025

Nr.	Projekt	Status	Fortschritt / Projektampel	Start	Ende
1	Einsetzung Sonderbeauftragter für Cyber-Außenpolitik und Cyber-Sicherheit	grün	100 %	30.4.2021	1.5.2021
2	Einrichtung Referat Cyberdiplomatie, sicherheitspolitische Aspekte neuer Technologien	grün	100 %	1.9.2020	1.7.2021
3	Verhandlungen VN-Cybercrimekonvention: Bereitstellung Junior Professional Officer für UNODC	grün	100 %	31.8.2021	31.12.2024
4	VN-Cybercrimekonvention: Reisekostenzuschuss für LDCs, LLDC, SIDS	grün	100 %	25.4.2021	31.12.2023
5	Teilnahme an Forschungs- und Entwicklungsprojekten	grün	95 %	31.8.2021	30.4.2025
6	Mitwirkung und Outreach in der International Counter Ransomware Initiative (CRI)	grün	60 %	29.10.2021	31.12.2099
7	Engagement in der OSZE für Public-Private Partnerships als VBM	grün	10 %	1.1.2018	31.12.2099
8	Engagement gegen den Missbrauch von kommerziellen Cyber-Intrusion-Tools	grün	5 %	22.9.2024	31.12.2099
9	VN Cybercrime-Konvention: Unterzeichnung/Ratifizierung/Umsetzung	grün	5 %	24.12.2024	31.12.2028

Projekt: Einsetzung Sonderbeauftragter für Cyber-Außenpolitik und Cyber-Sicherheit

Start: 30.4.2021
Ende: 1.5.2021
Nr.: 1032

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Gegenstand und Ziele

Geopolitische Spannungen finden stärker als zuvor auch im Cyberraum ihren Niederschlag.

Zur Stärkung der internationalen Zusammenarbeit ATs in Angelegenheiten der Cyberdiplomatie hat das BMEIA die Funktion eines Sonderbeauftragten für Cyber-Außenpolitik und Cyber-Sicherheit geschaffen. Zu seinen Aufgaben zählen die Delegationsleitung in multilateralen Verhandlungen und die Durchführung bilateraler Cyber-Dialoge sowie die Mitwirkung am EU-Netzwerk der Cyberbotschafter.

Beschreibung des Status

Der Sonderbeauftragte für Cyber-Außenpolitik und Cyber-Sicherheit hat seine Tätigkeit im Mai 2021 aufgenommen.

Organisationsfeld

BMEIA, II.2

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

Internationale Zusammenarbeit

Projekt: Einrichtung Referat Cyberdiplomatie, sicherheitspolitische Aspekte neuer Technologien

Start: 1.9.2020
Ende: 1.7.2021
Nr.: 1033

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

Ziel: Stärkung der internationalen Zusammenarbeit ATs in den Bereichen Cyberdiplomatie, hybride Bedrohungen und neue Technologien.

Die Aufgaben des in der Abteilung für sicherheitspolitische Angelegenheiten angesiedelten Referats umfassen: sicherheitspolitische Aspekte von Cybersicherheit, Cyberkriminalität, hybriden Bedrohungen und Desinformation sowie neuer Technologien; koordinierende Betreuung einschlägiger Aktivitäten im Rahmen der Vereinten Nationen (VN), der EU, des Europarates (EuR), der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) in Zusammenarbeit mit anderen befassten Ressorts; Vertretung des BMEIA in innerstaatlichen Gremien

Beschreibung des Status

Einrichtung eines neuen Referats Referat II.2.d „Cybersicherheit und Cyberkriminalität, Desinformation, hybride Bedrohungen“ per 1.9.2020

Umbenennung in Referat „Cyberdiplomatie und sicherheitspolitische Aspekte neuer Technologien“ per 1.7.2021

Organisationsfeld

BMEIA, II.2

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Cyberkriminalität und Strafverfolgung
- Internationale Zusammenarbeit

Projekt: Verhandlungen VN-Cybercrimekonvention: Bereitstellung Junior Professional Officer für UNODC

Start: 31.8.2021
Ende: 31.12.2024
Nr.: 1034

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

Das am Amtssitz Wien angesiedelte VN-Büro für Drogenbekämpfung und Verbrechensverhütung (UNODC) fungiert als Sekretariat des Ad hoc-Komitees zur Ausarbeitung eines umfassenden internationalen Übereinkommens über die Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken („VN-Cybercrimekonvention". Zur Unterstützung des UNODC in diesem für den Amtssitz Wien wichtigen Verhandlungsprozess finanziert das BMEIA die Stelle eines von AT bereitgestellten Junior Professional Officer (JPO)/Associate Expert im Bereich Cybercrimeprävention für die Dauer von zwei Jahren.

Beschreibung des Status

Die AT JPO-Stelle wurde im August 2021 besetzt. Nach einer Neuausschreibung aufgrund des Abgangs der früheren JPO wurde die Stelle Mitte Jänner 2023 neu besetzt und der JPO im Jänner 2024 um ein weiteres Jahr verlängert.

Organisationsfeld

BMEIA, II.5

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Internationale Zusammenarbeit
- Cyberkriminalität und Strafverfolgung

Projekt: VN-Cybercrimekonvention: Reisekostenzuschuss für LDCs, LLDC, SIDS

Start: 25.4.2021
Ende: 31.12.2023
Nr.: 1035

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

Seitens des BMEIA wurde UNODC ein Reisekostenzuschusses iHv € 200.000,– zur Teilnahme von LDCs, LLDCs und SIDS an den in Wien stattfindenden Tagungen des Ad-hoc Komitees zur Ausarbeitung einer VN-Cybercrimekonvention gewährt.

Beschreibung des Status

Überweisung des Reisekostenzuschusses iHv € 200.000,– an UNODC erfolgte nach Einrichtung eines entsprechenden Treuhandfonds im März 2022. Dieser wurde für die Teilnahme von Expert:innen aus LDCs an der 2., 4. und 5. Sitzung der Cybercrime-Verhandlungen in Wien (2022-2023) verwendet.

Organisationsfeld

BMEIA, I.4

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Cyberkriminalität und Strafverfolgung
- Internationale Zusammenarbeit

Projekt: Teilnahme an Forschungs- und Entwicklungsprojekten

Start: 31.8.2021
Ende: 30.4.2025
Nr.: 2096

Aktuelles Jahr
Status: grün
Fortschritt: 95 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- 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
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen
- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit

Gegenstand und Ziele

Unterstützung der AT Cybersicherheitsforschungslandschaft, insbesondere bei der Entwicklung praxisnaher Anwendungen

Beschreibung des Status

Das BMEIA nimmt aktuell an folgenden die Cybersicherheit betreffenden Projekten im Rahmen des AT Sicherheitsforschungsprogramms KIRAS teil:

- HYBRIS-Entwicklung einer Big Data/KI-Plattform zur Erkennung von hybriden Bedrohungen in sozialen Medien (mittels „Letter of Intent“)
- QCI-CAT (Quantum Communication Infrastructure – Secure Connectivity Austria; bis 05/25) – nationales AIT-Projekt im Rahmen des EuroQCI-Projekts zur Erstellung des ersten österreichweiten Quantenkommunikationsnetz für die sichere Kommunikation zwischen öffentlichen Behörden (als assoziierter Partner)

Organisationsfeld

BMEIA, II.2/VI.7

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

- Kleine und mittlere Unternehmen (KMU)
- Internationale Zusammenarbeit
- Widerstandsfähigkeit
- Forschung & Entwicklung
- Freier Meinungsbildungsprozess

Projekt: Mitwirkung und Outreach in der International Counter Ransomware Initiative (CRI)

Start: 29.10.2021
Ende: 31.12.2099
Nr.: 9173

Aktuelles Jahr
Status: grün
Fortschritt: 60 %

Zugrundeliegende Strategische Ziele

- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

Die International Counter Ransomware Initiative (CRI) wurde 2021 von den USA gestartet, um die internationale Zusammenarbeit bei der Bekämpfung von Ransomware-Kriminalität zu stärken. AT trat bereits kurz nach der Gründung bei und war bei den bisherigen vier Gipfeltreffen in Washington hochrangig vertreten. Aufgrund des transnationalen Charakters der Ransomware-Bedrohungen setzt sich das BMEIA im Rahmen des „Diplomacy and Capacity Building Pillar" für die Stärkung der internationalen Zusammenarbeit und Erweiterung der CRI-Mitglieder ein, insb. mit einem Fokus auf den Westbalkan.

Beschreibung des Status

Das CRI Leadership ging mit März 2025 an ein neues Steering Committee (SC, bestehend aus DE, UK, AU, SG) über. Im Zuge der Umstellung werden auch die Prioritäten evaluiert. AT/BMEIA setzt sich dabei in enger Zusammenarbeit mit dem SC (insbes. DE als Diplomacy Pillar Lead) dafür ein, regionalen Outreach und regionale Zusammenarbeit noch stärker als Schwerpunkt zu verankern. Ein Follow-Up zu den AT Outreach-Aktivitäten am Westbalkan ist in Planung.

Organisationsfeld

BMEIA, II.2

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Cyberkriminalität und Strafverfolgung
- Internationale Zusammenarbeit

Projekt: Engagement in der OSZE für Public-Private Partnerships als VBM

Start: 1.1.2018
Ende: 31.12.2099
Nr.: 9183

Aktuelles Jahr
Status: grün
Fortschritt: 10 %

Zugrundeliegende Strategische Ziele

- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;
- 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

Gegenstand und Ziele

Die OSZE Informal Working Group (IWG) zu Cybersicherheit hat 16 vertrauensbildende Maßnahmen (VBM) entwickelt, um das Risiko von Konflikten zwischen den Teilnehmerstaaten aufgrund der Nutzung von IKT zu verringern. AT bringt sich aktiv in die Arbeit der IWG ein, wobei ein besonderer Schwerpunkt auf CBM-14, Public-Private Partnerships liegt (gemeinsam mit BE, EE, FI, IT und SE).

Beschreibung des Status

BMEIA und BKA veranstalteten am 4. November 2024 ein Side-Event am Rande der IWG-Sitzung, um die Umsetzung von CBM-14/PPP in AT vorzustellen, u. a. CSP als zentrale Plattform für die Kooperation zwischen privatem und öffentlichem Sektor. Der Workshop war Auftakt zu einer Veranstaltungsserie, bei der die übrigen Mitglieder der CBM-14-Gruppe ihre nationalen Ansätze vorstellen (als nächstes FI im März 2025). AT wird sich weiterhin aktiv einbringen, um das Bewusstsein für die essenzielle Bedeutung von PPP im Cyberbereich zu stärken.

Organisationsfeld

BMEIA, II.2

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Internationale Zusammenarbeit
- Widerstandsfähigkeit
- Bewusstseinsbildung (Awareness)

Projekt: Engagement gegen den Missbrauch von kommerziellen Cyber-Intrusion-Tools

Start: 22.9.2024
Ende: 31.12.2099
Nr.: 9184

Aktuelles Jahr
Status: grün
Fortschritt: 5 %

Zugrundeliegende Strategische Ziele

- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

Der Missbrauch von kommerziellen Cyber-Intrusion-Tools und -diensten stellt ein wachsendes Sicherheitsrisiko dar. BMEIA beteiligt sich an internationalen Initiativen gleichgesinnter Partner zur Bewusstseinsbildung und Stärkung der Zusammenarbeit, um den illegitimen Einsatz derartiger Systeme zu unterbinden.

Beschreibung des Status

AT hat sich im September 2024 dem US-initiierten Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware angeschlossen.

BMEIA bringt sich aktiv in den derzeit laufenden, von FR und UK initiierten „Pall Mall Process“ ein, dessen Ziel es ist, einen „Code of Practice“ für den Umgang mit kommerziellen Cyber-Intrusion-Tools zu schaffen.

Organisationsfeld

BMEIA, II.2

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Internationale Zusammenarbeit
- Bewusstseinsbildung (Awareness)
- Vertrauen und Privatsphäre
- Widerstandsfähigkeit
- Cyberkriminalität und Strafverfolgung

Projekt: VN Cybercrime-Konvention: Unterzeichnung/Ratifizierung/Umsetzung

Start: 24.12.2024
Ende: 31.12.2028
Nr.: 9185

Aktuelles Jahr
Status: grün
Fortschritt: 5 %

Zugrundeliegende Strategische Ziele

- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;
- Österreich arbeitet in einem gesamtstaatlichen Ansatz stetig an der Weiterentwicklung seiner Rechtsgrundlagen zur Erhöhung der Cybersicherheit und Bekämpfung der Cyberkriminalität;

Gegenstand und Ziele

Die am 24.12.2024 von der VN-Generalversammlung angenommene Konvention stellt ein wichtiges Werkzeug im Kampf gegen Cyberkriminalität dar. AT hat sich von Anfang an aktiv in den zweieinhalb Jahre dauernden Verhandlungsprozess eingebracht. Besondere Anliegen waren uns u. a. hohe Menschenrechtsstandards, der Schutz von Kindern gegen sexuelle Ausbeutung und die Begrenzung der Konvention auf die wichtigsten Cyberverbrechen.

Beschreibung des Status

Die Konvention wird ab Mitte 2025 zur Unterzeichnung aufliegen. Da es sich um einen gesetzesändernden Staatsvertrag handelt, bedarf die innerstaatliche Ratifikation der Genehmigung des Nationalrates. Parallel zu diesem nationalen Prozess wird auch auf EU-Ebene das Verfahren zum Beitritt der EU (gemischtes Abkommen) durchzuführen sein. BMEIA wird beide Prozesse begleiten und mit den fachlich zuständigen Ressorts (insb. BMJ) koordinieren.

Organisationsfeld

BMEIA, II.2

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Cyberkriminalität und Strafverfolgung
- Internationale Zusammenarbeit

BMAW

Projektverantwortliches Ressort
Bundesministerium für Arbeit und Wirtschaft

Stand: 5.3.2025

Nr.	Projekt	Status	Fortschritt / Projektampel	Start	Ende
1	[BEV] Zusätzliche Ressourcen für den Schutz der kritischen Infrastruktur	grün		1.1.2021	31.12.2023
2	[BEV] GAP-Analyse zur Informationssicherheit	grün	1 %	18.9.2021	31.12.2023
3	[Sektion VI] Cybersicherheit in der dualen Berufsausbildung	grün	100 %	1.12.2020	31.12.2023
4	[PRÄS] Konzept für Cybersicherheits-Berichtswesen (IKT-W)	grün	100 %	1.1.2022	31.5.2024
5	[PRÄS] Überprüfung der IT-Sicherheitsmechanismen 2021 für den BMDW-Standardarbeitsplatz (IKT-W)	grün	100 %	20.1.2023	28.4.2022
6	[PRÄS] Etablierung einer IT-Notfall-Organisation (IKT-W)	grün	100 %	29.7.2021	27.6.2022
7	[Sektion IV] Förderungsprogramm „KMU.Cybersecurity“	grün	100 %	1.4.2022	30.4.2024
8	[PRÄS] Aktualisierung der InfoSih-Richtlinie (IKT-W)	grün	100 %	30.4.2023	31.5.2024
9	[PRÄS] Überprüfung der IT-Sicherheitsmechanismen 2023 (IKT-W)	grün	100 %	1.6.2023	29.2.2024
10	[PRÄS] Überprüfung der IT-Sicherheitsmechanismen 2024 für den BMAW-Standardarbeitsplatz (IKT-W)	grün	100 %	1.11.2024	28.2.2025

Projekt: [BEV] Zusätzliche Ressourcen für den Schutz der kritischen Infrastruktur

Start: 1.1.2021
Ende: 31.12.2023
Nr.: 4109

Aktuelles Jahr
Status: grün
Fortschritt: 0 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen

Gegenstand und Ziele

Es sollen zum Schutz von kritischer Infrastruktur (Beispiel BEV: Kataster, APOS) mehr finanzielle und personelle Ressourcen bereitgestellt werden. Insbesondere der Kataster ist (wie das Grundbuch) für die Sicherung an Eigentum für den Wirtschaftsstandort unersetzlich.

Beschreibung des Status

Noch nicht gestartet (hängt mit Maßnahme „GAP-Analyse zur Informationssicherheit“ zusammen)

Organisationsfeld

BMAW (BEV)

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Widerstandsfähigkeit

Projekt: [BEV] GAP-Analyse zur Informationssicherheit

Start: 18.9.2021
Ende: 31.12.2023
Nr.: 4110

Aktuelles Jahr
Status: grün
Fortschritt: 1%

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen

Gegenstand und Ziele

Es wird eine Analyse in Form eines externen Audits zur Ermittlung des Sicherheitsniveaus der IT-Architekturkomponenten im BEV durchgeführt. Nach Analyse des Status-Quo des IT-Sicherheitslevels bzw. nach Vorliegen der einzelnen erforderlichen Handlungsfelder können sodann weitere Maßnahmen im Hinblick auf die Cybersicherheit abgeleitet werden.

Beschreibung des Status

GAP-Analyse bereits durchgeführt

Organisationsfeld

BMAW (BEV)

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Wirtschaftsstandort

Projekt: [Sektion VI] Cybersicherheit in der dualen Berufsausbildung

Start: 1.12.2020
Ende: 31.12.2023
Nr.: 4111

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

Digitale Kompetenzen sind noch nicht systematisch in den Ausbildungsordnungen von Lehrberufen enthalten. Grundlegende digitale Kompetenzen können unter den transvesalen Kompetenzen subsumiert werden. Transversale Kompetenzen umfassen Kenntnisse und Fertigkeiten, die in jedem Lehrberuf gleichermaßen von Bedeutung für die Berufsausübung sind. Hierzu zählen auch die transversalen digitalen Kompetenzen, die ein grundlegendes Wissen um Cybersecurity umfassen.

Beschreibung des Status

Im Rahmen eines Projekts der Sozialpartner und des BMAW wurden transversale (digitalen) Kompetenzen und deren strukturelle Integration in die Ausbildung von Lehrberufen betrachtet. Die Aufnahme von transversalen Kompetenzen inklusive der transversalen digitalen Kompetenzen in Form von fachübergreifenden Kompetenzen (Arbeiten im betrieblichen und beruflichen Umfeld; Qualitätsorientiertes, sicheres und nachhaltiges Arbeiten; Digitales Arbeiten) in jedes neu erlassene Berufsbild der dualen Berufsausbildung ist mittlerweile Standard.

Organisationsfeld

BMAW (VI/7)

Herausforderungen

- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Bewusstseinsbildung (Awareness)
- Bildung

Projekt: [PRÄS] Konzept für Cybersicherheits-Berichtswesen (IKT-W)

Start: 1.1.2022
Ende: 31.5.2024
Nr.: 4112

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen

Gegenstand und Ziele

Die IKT-Verfahren des BMAW (VerwB Wirtschaft) werden in unterschiedlichen Rechenzentren – mit unterschiedlichen Sicherheitsmonitoringsystemen – betrieben.

Im Rahmen dieser Aktivität ist ein einheitlicheres Berichtswesen – unter Berücksichtigung der unterschiedlichen technischen Lösungen – zu konzipieren.

Beschreibung des Status

Für die meisten IKT-Verfahren (inkl. dem wichtigen Standard-arbeitsplatz-IT-Verfahren) ist bereits eine zyklisches und sehr granulares Berichtswesen installiert.

Mit der im Mai 2024 erlassenen InfoSih-Richtlinie wurde ein generelles Berichtswesen festgelegt & so auch in der Praxis etabliert.

Organisationsfeld

BMAW (Präs/11)

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

Widerstandsfähigkeit

Projekt: [PRÄS] Überprüfung der IT-Sicherheits-mechanismen 2021 für den BMDW-Standardarbeitsplatz (IKT-W)

Start: 20.1.2023
Ende: 28.4.2022
Nr.: 4113

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen

Gegenstand und Ziele

Im Rahmen eines IT-Security-Audits soll durch unabhängige Experten die externen Schwachstellen & Zugriffsmöglichkeiten gefunden und aktuelle Angriffsmethoden angewandt werden und allfällige Optimierungen vorgeschlagen werden. Ebenso soll die IT-Security-Awareness der Benutzer durch gängige Kampagnen (Phishing etc.) verifiziert werden.

Beschreibung des Status

Das Audit startete im Dezember 2021. Alle 3 Module/Überprüfungen (technisch intern, technisch extern/social-physical) wurden mit 14.01.2022 abgeschlossen. Der Abschlussbericht wurde planmäßig im Februar fertigerstellt & übergeben. Die Bearbeitung der Findindings erfolgt über ein gesondertes Action Item.

Organisationsfeld

BMAW (Präs/11)

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

Widerstandsfähigkeit

Projekt: [PRÄS] Etablierung einer IT-Notfall-Organisation (IKT-W)

Start: 29.7.2021
Ende: 27.6.2022
Nr.: 4114

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen

Gegenstand und Ziele

Um für den Eintritt von IT-Notfällen bestmöglich gewappnet zu sein, soll ein IT-Notfallhandbuch, welches auch Szenarien für Cybersicherheitsbedrohungen berücksichtigt, erstellt werden. In diesem Sammelwerk ist neben dem organisatorischen Aufbau, der prozessuale Ablauf, die möglichen Eintrittsszenarien sowie auch die jeweiligen Abwehr- und Wiederherstellungsmaßnahmen zu definieren.

Beschreibung des Status

Das allgemeine Krisenhandbuch des Ressorts wurde im Jänner 2022 überarbeitet und der spezielle Abschnitt zum Lagebild „Cyber Angriff“ seitens IKT im Februar 2022 aktualisiert & integriert. Neben der generellen Beschreibung des Lagebildes wurden zudem auch ergänzende Dokumente & Leitfäden (Kontakteliste, Einsatzleiterreihenfolge, Wiederanlaufplan, Wiederaufbauplan, CERT-Setup) erarbeitet und als Appendixe angefügt.

Organisationsfeld

BMAW (Präs/11)

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

Widerstandsfähigkeit

Projekt: [Sektion IV] Förderungsprogramm „KMU.Cybersecurity“

Start: 1.4.2022
Ende: 30.4.2024
Nr.: 4115

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- 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
- Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten

Gegenstand und Ziele

Die Zahl an Cyberangriffen auf Firmennetzwerken nimmt stetig zu. Eine weitere Verschärfung ist durch den Ukraine-Krieg zu erwarten. Das BMDW legt daher ein Förderungsprogramm auf, um Cybersicherheitsmaßnahmen in KMU-Bereich zu forcieren.

Eckdaten zum Programm:

- Budget von 2,3 Mio. Euro
- Förderbar sind Investitionen, Beratungsleistungen, Kosten externer Anbieter (z. B. Lizenzgebühren) für max. 18 Monate
- Projektkosten zwischen 2.000 und 50.000 Euro sind förderbar
- Fördersatz von bis zu 40 %, d. h. max. Förderung von 20.000 Euro

Beschreibung des Status

Die Ausschreibung startete am 01.04.2022 und musste nach rund 10 Tagen aufgrund Budgetausschöpfung geschlossen werden. Insgesamt gingen 282 Anträge ein, wovon schließlich 191 Projekte mit einem ausbezahlten Zuschussvolumen von rd. EUR 1,6 Mio. gefördert wurden.

Organisationsfeld

BMAW (IV/4)

Herausforderungen

- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

Kleine und mittlere Unternehmen (KMU)

Projekt: [PRÄS] Aktualisierung der InfoSih-Richtlinie (IKT-W)

Start: 30.4.2023
Ende: 31.5.2024
Nr.: 6128

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen

Gegenstand und Ziele

Die bestehende InfoSih-Richtlinie ist generell zu überarbeiten und an die aktuellen Gegebenheiten aber auch erforderlichen und absehbaren Anforderungen anzupassen.

Beschreibung des Status

Die generelle Überarbeitung der InfoSih-Richtlinie ist erfolgt und alle relevanten Anpassungsnotwendigkeiten (State-of-the-Art Vorgehen, weitreichende Governance, CISO, ISMS, Rechte & Pflichten etc.) sind enthalten. Die neue Richtlinie wurde im Mai 2024 im gesamten Ressort erlassen.

Organisationsfeld

BMAW (Präs/11)

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Cyberverteidigung

Projekt: [PRÄS] Überprüfung der IT-Sicherheits-mechanismen 2023 (IKT-W)

Start: 1.6.2023
Ende: 29.2.2024
Nr.: 6129

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen

Gegenstand und Ziele

Im Rahmen eines Security-Audits soll das IT-Verfahren „Standardarbeitsplatz“ durch unabhängige Experten auf Schwachstellen und Zugriffsmöglichkeiten analysiert und aktuelle Angriffsmethoden angewandt werden. Im Zuge des Audits sind nicht nur die externen Services zu überprüfen sondern auch die gesamte IKT-Infrastruktur von intern zu analysieren.

In einem Ergebnisbericht sind abschließend sämtliche Erkenntnisse festzuhalten sowie Verbesserungsvorschläge auszuformulieren.

Beschreibung des Status

Anhand des BBG-Los „Cybersicherheits-Dienstleistungen“ wurden mit dem erstgereihten Security-Dienstleister eine technische Sicherheitsüberprüfung konzipiert und bestellt. Das Audit wurde im Dezember 2023 abgeschlossen, der Ergebnisbericht übermittelt und die Präsentation sowie der Technik-Workshop durchgeführt.

Organisationsfeld

BMAW (Präs/11)

Herausforderungen

- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Cyberverteidigung

Projekt: [PRÄS] Überprüfung der IT-Sicherheits-mechanismen 2024 für den BMAW-Standardarbeitsplatz (IKT-W)

Start: 1.11.2024
Ende: 28.2.2025
Nr.: 9175

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren

Gegenstand und Ziele

Im Rahmen eines IT-Security-Audits soll durch unabhängige Experten die Widerstandsfähigkeit definierter IKT-Verfahren des BMAW (VerwB Wirtschaft) überprüft werden. Im Zuge dessen sind u. a. Schwachstellen, Zugriffs- & Angriffsmöglichkeiten bei den exponierten Services aber auch der gesamten internen IKT-Infrastruktur gefunden und allfällige Optimierungen vorgeschlagen werden.

Beschreibung des Status

Die technische Sicherheitsüberprüfung wurde im November & Dezember 2024 durchgeführt. Der Ergebnisbericht wurde im Jänner 2025 erstellt und übermittelt. Im Zuge darauffolgender Workshops wurden alle Empfehlungen gemeinsam aufgearbeitet und alle sinnvollen/treffsicheren Maßnahmen in einen Maßnahmenkatalog extrahiert. Die Abarbeitung der einzelnen Maßnahmen findet – priorisiert nach dem Schwachstellenschweregrad – im Zuge der Betriebsführung statt.

Organisationsfeld

BMAW (Präs/11)

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Cyberverteidigung

BMSGPK

Projektverantwortliches Ressort

Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz

Stand: 5.3.2025

Nr.	Projekt	Status	Fortschritt / Projektampel	Start	Ende
1	IT-System zur Erkennung von sicherheitskritischen Ereignissen (SIEM) gemäß Etappenplan	grün	85 %	1.2.2023	31.12.2025
2	Etablierung Leitlinien Risikomgmt. in der Netz- und Informationssicherheit	grün	100 %	1.2.2023	20.12.2024
3	Weiterentwicklung des Informationssicherheitsmanagement (ISMS) Tools	grün	80 %	1.2.2023	31.12.2025
4	Erstellung eines Maßnahmenplans zur Netz- und Informationssicherheit	grün	80 %	1.1.2024	30.6.2025

Projekt: IT-System zur Erkennung von sicherheitskritischen Ereignissen (SIEM) gemäß Etappenplan

Start: 1.2.2023
Ende: 31.12.2025
Nr.: 6120

Aktuelles Jahr
Status: grün
Fortschritt: 85 %

Zugrundeliegende Strategische Ziele

Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen

Gegenstand und Ziele

Ziel ist die in der österreichischen Strategie für Cybersicherheit im Jahr 2021 festgelegten Herausforderungen zur missbräuchlichen Verwendung von IT-Systemen zu adressieren, um Cyberkriminalität durch Angreifende mit einem Security Information and Event Management (SIEM) System bekämpfen zu können. Etablierte Lösungen des Bundes stehen im Fokus, um größtmögliche Synergiepotentiale nutzen zu können. Dabei wird der von der DSGVO geforderte „Stand der Technik" für die Sicherheit der Verarbeitung zur Etablierung eines angemessenen Schutzniveaus durch das SIEM verbessert.

Beschreibung des Status

Status 01.02.2023: Service- und Produktentscheidung getroffen; Vorbereitung von Sicherheits- und Datenschutzanforderungen.

Status 15.05.2023: Freigabe zum Einsatz des SIEM-Systems an den IT Service Provider erfolgt. Die ersten Shared-Services wurden in Betrieb genommen.

Status 26.07.2023: Anforderung eines Dashboards für Infrastruktur-KPIs beim IT Service Provider.

Status 26.02.2024: Angebot des IT Providers zum Ausbau des SIEM zu mittels Security Analysten liegt vor.

Status 01.08.2024: Angebot des IT Providers zur Etablierung der Rolle „Security Analyst" wurde beauftragt.

Status 25.02.2025: Weiterentwicklung von Anwendungsfällen ist gestartet.

Organisationsfeld

BMSGPK I/B/8

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Cyberkriminalität und Strafverfolgung
- Cyberverteidigung

Projekt: Etablierung Leitlinien Risikomgmt. in der Netz- und Informationssicherheit

Start: 1.2.2023
Ende: 20.12.2024
Nr.: 6121

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

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

Gegenstand und Ziele

Ziel ist die in der österreichischen Strategie für Cybersicherheit im Jahr 2021 festgelegten Herausforderungen zu Abhängigkeiten von IT und künftige technologische Entwicklungen mittels eines angemessenes Risikomanagements für IT-Sicherheit zu adressieren. Das Organisationshandbuch zum Management von Risiken in der IT-Sicherheit wird als eigenständiges Dokument zusätzlich zur bestehenden BMSGPK IT-Sicherheitspolitik im ISMS ergänzt. Im Fokus steht die adäquate Umgangsstrategie mit dem Risiko (Vermeidung, Modifikation, Streuung, Akzeptanz) und die transparente Dokumentation inkl. Berichterstattung.

Beschreibung des Status

Status 01.02.2023:

Vorhaben in der Sitzung des Sicherheitsmanagement-Teams vorgestellt; Ausrichtung nach der Norm ISO/IEC 27005 festgelegt.

Status 15.05.2023:

Entwurf einer Berechnungsmethode zur Risikobewertung sowie eines Organisationshandbuches fertiggestellt. Abstimmungsprozess gestartet.

Status 26.07.2023:

Evaluierung eines Tools für Risikomanagement in der Informationssicherheit.

Status 26.02.2024:

Toolentscheidung hinsichtlich BMF Reporting Plattform getroffen, Prozess zur Risikoerhebung 2024 gestartet.

Status 01.08.2024:

Risikoerhebung 2024 wurde durchgeführt, Risikolandkarte ist in Erstellung.

Status 25.02.2025:

Berichtslegung 2024 ist erfolgt.

Organisationsfeld

BMSGPK I/B/8

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Cyberverteidigung
- Bewusstseinsbildung (Awareness)
- Vertrauen und Privatsphäre

Projekt: Weiterentwicklung des Informationssicherheits-management (ISMS) Tools

Start: 1.2.2023
Ende: 31.12.2025
Nr.: 6122

Aktuelles Jahr
Status: grün
Fortschritt: 80 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

Das bereits eingesetzte ISMS-Tool soll hinsichtlich der Schutzbedarfsfeststellung für kritische Anwendungen/Services mit einer verfeinerten Klassifikation des IT Security Asset Managements (z. B. Differenzierung zwischen Fach- und Querschnittsanwendung sowie Basis IT-Service) erweitert werden. Die bereits vorhandenen Intrusion Prevention System (IPS) Berichte sollen analog dem bestehenden Prozess für den Security Management Report (SMR) in das ISMS-Tool integriert und monatlich zur Verfügung gestellt werden. Erweiterung diverser Sicherheitskonzepte für IT-Anwendungen.

Beschreibung des Status

Status 01.02.2023: Beauftragung für 2023 ist erfolgt und die Anforderungen wurden an den IT Service Provider kommuniziert.

Status 27.06.2023: Neue Funktion im ISMS zum monatlichen Mail-Versand von offen IT-Sicherheitsprüfungen an den IT Systemverantwortlichen wurde aktiviert.

Status 26.07.2023: E-Mail Schnittstelle zum Import von Sicherheitsberichten (ins. des Intrusion Prevention System – IPS) wurde technisch ausgearbeitet.

Status 26.02.2024: E-Mail Schnittstelle zur Integration des IPS umgesetzt. Migration auf ein Shared Service beauftragt.

Status 01.08.2024: Diverse Weiterentwicklungen, z. B. E-Mail Reminder und Statistische Auswertungen, wurden für das ISMS beauftragt.

Status 25.02.2024: Digitalisierung des Prozesses zur Schutzbedarfsfeststellung (SBF).

Organisationsfeld

BMSGPK I/B/8

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Vertrauen und Privatsphäre
- Cyberverteidigung

Projekt: Erstellung eines Maßnahmenplans zur Netz- und Informationssicherheit

Start: 1.1.2024
Ende: 30.6.2025
Nr.: 8153

Aktuelles Jahr
Status: grün
Fortschritt: 80 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren

Gegenstand und Ziele

Ziel ist die Aufsetzung einer GAP-Analyse, Reifegradfeststellung, Zielbilddarstellung sowie die Erstellung eines umfangreichen Maßnahmenkatalogs zur Sicherstellung und Wahrung der Anforderungskonformität im Bereich der Netz- und Informationssicherheit.

Vorgeschichte 1. HJ 2024:

02.01.24: Festlegung des Projektteams und des zu betrachtenden Scopes

18.01.24: Erstellung und Freigabe des Projektauftrages

01.02.24: Inkraftsetzung einer Grobkostenstruktur sowie einer zentralen Datei- und Dokumentenablage

15.02.24: Identifizierung erster Prüfmechanismen und -maßnahmen für die Errichtung einer vollumfänglichen GAP-Analyse

15.03.24: Absolvierung des ressortübergreifenden Assessments „Security Framework Bund“ (SFB)

Beschreibung des Status

18.07.24: Fertigstellung der Ersteinschätzungs-Plausibilitätsvalidierung in Zusammenarbeit mit den SFB-Projektmitwirkenden

31.07.24: Aufsetzung des aus der GAP-Analyse entstandenen Maßnahmenkatalogs

15.08.24: Priorisierende Einordnung der ermittelten Behandlungspunkte

23.09.24: Feststellung der Verzögerung des nationalen Gesetzestextes

07.10.24: Anstoßen des Lieferantenmanagements samt erster Auditierungen

21.11.24: Verschärfungen des Präventivumfangs in Sachen Gewährleistung Infrastrukturbetrieb

Organisationsfeld

VI/B/10

Herausforderungen

- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

Widerstandsfähigkeit

CSP/PPP

Projektverantwortliches Ressort

Cyber Sicherheit Plattform/Public Private Partnership

Stand: 5.3.2025

Nr.	Projekt	Status	Fortschritt / Projektampel	Start	Ende
1	A1 Seniorenakademie	grün	100 %	31.3.2021	31.12.2099
2	AIT – Fake Shop Detector (FSD)	grün	60 %	1.1.2024	24.12.2026
3	AIT – Kampf gegen Desinformation	grün	60 %	1.1.2024	24.12.2026
4	OeNB – Off-Site Analyse bei österreichischen LSI	grün	100 %	30.11.2017	31.12.2099
5	OeNB – DORA-Implementierung für die LSI Off-Site Analyse	grün	65 %	1.7.2024	31.12.2026
6	FH JOANNEUM – TRANSFORM	grün	80 %	1.1.2024	30.8.2025
7	SBA Security Advisories	grün	100 %	1.1.2020	31.12.2099
8	FH OÖ F&E GmbH – Cybersecurity Forschung	grün	100 %	1.10.2009	31.12.2099
9	FH JOANNEUM – Go Cloud Go Secure	grün	10 %	1.11.2024	30.10.2026
10	FH JOANNEUM – RADIUS	grün	5 %	1.1.2025	31.12.2029
11	OeNB, FMA – TIBER-AT Implementation	grün	85 %	1.8.2024	30.9.2025
12	AIT – KI-basierte Technologien für effektive Cyber Security Schutzmaßnahmen	grün	60 %	1.1.2024	31.12.2026
13	AIT/GAIA-X – wiki.ATLAWS.eu	grün	80 %	1.1.2024	31.12.2026
14	AIT – Internationales Digital Security Forum (IDSF)	grün	80 %	1.1.2023	31.12.2027
15	AIT/KSÖ – nationales Cyber Security Planspiel mit Behörden und KRITIS	grün	80 %	1.1.2023	31.12.2027
16	A1 Seniorenakademie in A1 Shops	grün	100 %	1.1.2023	31.12.2099
17	A1 digital.campus	grün	100 %	1.1.2020	31.12.2099
18	A1 digital.campus – MINT & Engineering Fokus	grün	10 %	19.2.2024	31.12.2099
19	Uni Wien – DaTra	grün	100 %	1.12.2022	31.1.2024
20	SBA – ASOC	grün	30 %	1.1.2024	1.1.2026
21	FMA,OENB – TIBER AT Framework	grün	100 %	6.4.2021	31.12.2023
22	FMA, OeNB – Threat Led Penetration Testing	grün	85 %	1.1.2023	31.12.2099
23	KSÖ – Baseline Cybersecurity Standard für KMUs	grün	60 %	27.1.2021	31.3.2023
24	FH OÖ – Fachhochschulausbildung in Informationssicherheit	grün	100 %	31.8.2000	31.12.2099
25	WKÖ – IT-SAFE	grün	100 %	1.1.2022	31.12.2099
26	WKÖ – CYBER SECURITY HOTLINE WKO	grün	100 %	1.1.2022	31.12.2099
27	WKÖ – CYBER SECURITY FEUERWEHR WKO	gelb	20 %	1.1.2022	31.12.2099

Nr.	Projekt	Status	Fortschritt / Projektampel	Start	Ende
28	WKÖ – Women4Cyber Austria	grün	100 %	31.8.2022	31.12.2099
29	VERBUND – OT Cyber Security Lab	grün	100 %	14.6.2020	31.12.2023
30	COMPARO – OPSAM Community Edition: zentrale Wissens-drehscheibe Cybersicherheit	grün	100 %	30.9.2021	31.12.2025
31	DVC – Trainingskurs OPCYBRES: Cybersicherheit als Eckpfeiler der Unternehmensresilienz	grün	100 %	1.11.2021	31.12.2099
32	KPMG/KSÖ-Cybersicherheitsstudie „Cybersecurity in Österreich“	grün	20 %	1.8.2024	30.6.2025
33	KPMG – Cyber Awareness Monat Oktober 2024: Sensibilisierung und Trainings	grün	40 %	31.5.2024	31.12.2024
34	INDUCE Cyber Security Literacy And Dexterity through Cyber Exercises	grün	30 %	1.4.2021	31.3.2024
35	AIT – Post-Quanten-Computer sichere Verschlüsselung für höchste Cyber Sicherheit	grün	70 %	1.1.2021	31.12.2026
36	AIT – Ausbau der Cyber-Security Widerstandsfähigkeit für kritische Infrastrukturbetreiber in AT	grün	95 %	1.1.2021	31.12.2026
37	Learners – effizientere Methodologien + Methodiken komplexe und Dynamische Inhalte für Jugend	gelb	4 %	1.4.2022	31.12.2023
38	Nationales Cyber Security Trainingszentrum	gelb	2 %	31.8.2022	31.12.2025
39	VISP – Vienna InternetSecurityPrivacy Cluster	grün	100 %	1.3.2020	31.12.2099
40	OCG – Young Researchers Day	grün	100 %	1.3.2024	31.12.2099
41	CSA – HackFu	grün	15 %	30.9.2022	29.9.2023
42	„Shecurity“ – Hackerinnen Training	grün	100 %	31.5.2023	31.12.2099
43	SBA, sec4dev – youTube Kanal	grün	100 %	4.9.2015	31.12.2099
44	SBA, ÖIAT – Security Awareness Stammtisch	grün	100 %	24.4.2023	31.12.2099
45	SBA – Cybersecurity Quiz	grün	100 %	30.9.2021	31.12.2099
46	SBA – securepizza.club @ SBA Research	grün	100 %	1.1.2021	31.12.2099
47	SBA – Women in Privacy & Security Vienna	grün	100 %	1.1.2021	31.12.2099
48	SBA – Seurity Meetup	grün	100 %	1.1.2021	31.12.2099
49	ISPA – Der Online-Zoo	grün	75 %	1.12.2015	1.7.2025
50	ACSC – Austrian Cyber Security Challenge 2023	grün	60 %	1.1.2023	31.12.2023
51	ECSC – European Cyber Security Challenge 2023	grün	50 %	1.1.2023	31.12.2023
52	openECSC – Open European Cyber Security Challenge 2023	grün	35 %	20.1.2023	31.12.2023
53	FH OÖ – SSCCS (Secure Supply Chains for critical systems)	grün	80 %	30.6.2021	31.12.2024
54	FH OÖ – CySeReS-KMU	grün	70 %	1.1.2023	30.6.2025
55	FH OÖ – Sucredi	grün	100 %	1.1.2019	29.6.2022
56	AIT -Aufbau von Übungs- und Trainingsplattformen für Multistakeholder Infrastrukturszenarien	grün	70 %	30.9.2022	31.12.2024
57	AIT – Realisierung von Cyber Security Schlüsseltechnologien made in Austria mit globalem Impact	grün	90 %	1.1.2022	31.12.2025

Nr.	Projekt	Status	Fortschritt / Projektampel	Start	Ende
58	AIT – Beitrag Österreichs zur Umsetzung des EU Cyber Resilience Acts	grün	70 %	1.1.2022	31.12.2026
59	AIT – Aufbau effektiver Threat-Intelligence Fähigkeiten für den Wirtschaftsstandort Österreich	grün	60 %	1.1.2022	31.12.2026
60	Mindsetters – Cyber-Awareness für Österreich – Produktname: „2b-aware“	grün	100 %	31.7.2022	1.5.2024
61	AKNOe -Onlinebetrug-Simulator	grün	100 %	1.7.2021	30.6.2022
62	epicenter.academy: Digitale Selbstverteidigung	grün	50 %	12.12.2022	1.7.2028
63	AIT – Österreich als aktiver EU Cyber Security Skill Development Stakeholder	grün	10 %	1.6.2023	31.12.2026
64	SV – Weiterentwicklung SV-Sicherheitsstandards	grün	80 %	1.10.2022	31.3.2024
65	FH JOANNEUM – Masterstudium IT & Mobile Security	grün	100 %	1.1.2001	31.12.2099
66	FH JOANNEUM – CyMoDACS: Cyber-Security and Mobility for Digital Aeronautic Communication Systems	grün	80 %	1.1.2022	30.6.2025
67	FH JOANNEUM – CSecTOR	grün	100 %	1.12.2022	30.11.2024

Projekt: A1 Seniorenakademie

Start: 31.3.2021
Ende: 31.12.2099
Nr.: 2066

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

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

Gegenstand und Ziele

Die A1 Seniorenakademie ist eine Schulungsinitiative in Kooperation mit dem Österreichischen Seniorenrat, die sich speziell an die Generation 60+ richtet. In kostenlosen Kursen für Anfänger und Fortgeschrittene helfen erfahrene Trainer:innen, sich im Internet sicher zurecht zu finden. Die Kurse werden österreichweit – insbesondere in kleinen Gemeinden – sowie Online angeboten.

Schulungsthemen sind u. a.: Erste Schritte im Internet, Suchen und Finden mit Google, Kommunikation mit WhatsApp und Email, Videotelefonie mit Smartphone und Tablet, Einrichten von WLAN. Besonderes Augenmerk wird auf die Sicherheit und den Schutz der Privatsphäre gelegt.

Beschreibung des Status

Das aktuelle Programm ist abrufbar über die Seite: https://A1Seniorenakademie.at/.

Das BMSAGK zeichnete dieses Programm im März 2022 mit dem Gütesiegel „Digitale Senior:innen Ausbildung“ aus.

Organisationsfeld

A1 Telekom Austria AG

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Vertrauen und Privatsphäre
- Bewusstseinsbildung (Awareness)

Projekt: AIT – Fake Shop Detector (FSD)

Start: 1.1.2024
Ende: 24.12.2026
Nr.: 9166

Aktuelles Jahr
Status: grün
Fortschritt: 60 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen

Gegenstand und Ziele

Beitrag zur digitalen Souveränität der Online-Kunden in Österreich. Digitaler Cyber Crime Konsumentenschutz.

Beschreibung des Status

Implimentierung und Service-Angebot eines modernen KI-basierten Cyber Crime Schutzwerkzeuges für Online-Kund:innen. Staatspreis 2024, AV-Testsieger im internationalen Vergleich. Etablierte Kooperation mit dem Justizministerium Bayern

Organisationsfeld

AIT Austrian Institute of Technology, Center for Digital Safety & Security

Herausforderungen

- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Cyberkriminalität und Strafverfolgung
- Vertrauen und Privatsphäre

Projekt: AIT – Kampf gegen Desinformation

Start: 1.1.2024
Ende: 24.12.2026
Nr.: 9167

Aktuelles Jahr
Status: grün
Fortschritt: 60 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen

Gegenstand und Ziele

Kompetenzen und Werkzeuge für den effektiven Kampf gegen Desinformation und hybriden Bedrohungen

Beschreibung des Status

Entwicklung von dedizierten OSINT Kompetenzen und Ressourcen und neue KI basierte Technologien und Werkzeugen in Österreichen um einen effektiven Schutz vor Desinformation und hybriden Bedrohungen zu schützen. nationaler Beitrag zur Stärkung der Fähigkeiten der österr. Behörden. Nationale gesamtstaatliche Übungen durchgeführt. etablierte Kooperationen im Medienbereich mit APA. DPA und AFP

Organisationsfeld

AIT Austrian Institute of Technology, Center for Digital Safety & Security

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Vertrauen und Privatsphäre
- Freier Meinungsbildungsprozess
- Widerstandsfähigkeit
- Cyberverteidigung

Projekt: OeNB – Off-Site Analyse bei österreichischen LSI

Start: 30.11.2017
Ende: 31.12.2099
Nr.: 9168

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- 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

Gegenstand und Ziele

Laufende Off-Site Analyse über österreichische LSI hinsichtlich IT-Risiko und Informationssicherheit (im Rahmen des operationellen Risikos). Kontinuierliche Weiterentwicklung und Anpassung.

Beschreibung des Status

- Risikobasierte laufende Analyse österr. LSI mit Schwerpunkt auf IT-Risiko und Informationssicherheit im Rahmen des operationellen Risikos
- Die zentralen regulatorischen Vorgaben stellen bis 16.01.25 die EBA Leitlinien EBA/GL/2017/05 (ergänzt durch EBA/GL/2019/04) sowie die EZB-Vorgaben (u. a. LSI SREP Methodologie) dar
- Anpassung der regulatorischen Vorgaben ab 17.01.25 auf DORA

(laufende Tätigkeit, bleibt als Aktivität bestehen)

Organisationsfeld

OeNB

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Widerstandsfähigkeit

Projekt: OeNB – DORA-Implementierung für die LSI Off-Site Analyse

Start: 1.7.2024
Ende: 31.12.2026
Nr.: 9169

Aktuelles Jahr
Status: grün
Fortschritt: 65 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- 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

Gegenstand und Ziele

Ab Jänner 2025 gelten die Vorgaben über die digitale operationale Resilienz im Finanzsektor (DORA). Bei den österreichischen LSI soll das Bewusstsein für die kommenden Anforderungen geschaffen werden.

Die erforderlichen Umsetzungsschritte („Gaps“) zur künftigen aufsichtlichen Überprüfung der Einhaltung von DORA-Vorgaben durch die österreichischen LSI werden ermittelt und folgend proportional, risikoadäquat und in Abstimmung mit der EZB/dem SSM implementiert.

Beschreibung des Status

- Mitwirkung bei Vorträgen und Informationsveranstaltungen um österreichische LSI hinsichtlich der DORA Anforderungen zu sensibilisieren
- Durchführung einer DORA-Gap Analyse, als Ausgangspunkt werden die EBA Leitlinien EBA/GL/2017/05 sowie die derzeitigen EZB-Vorgaben herangezogen.
- Aufsichtsseitige Implementierung der durch die DORA-Gap Analyse aufgezeigten Handlungsfelder (derzeit ist eine zweistufige Ausrollung 2025 und 2026 angedacht, um in Abstimmung mit der EZB bzw. dem SSM vorgehen zu können)

Organisationsfeld

OeNB

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Widerstandsfähigkeit

Projekt: FH JOANNEUM – TRANSFORM

Start: 1.1.2024
Ende: 30.8.2025
Nr.: 9170

Aktuelles Jahr
Status: grün
Fortschritt: 80 %

Beschreibung des Status

Laufende Trainings und Workshops für Unternehmen im Bereich Cyber Security und Data Analytics

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen
- 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

Gegenstand und Ziele

FFG – Innovationcamps Ausschreibung 2022, Cyber Security + Data Science

Organisationsfeld

FH JOANNEUM Institut Software Design & Security

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Bewusstseinsbildung (Awareness)

Projekt: SBA Security Advisories

Start: 1.1.2020
Ende: 31.12.2099
Nr.: 9171

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

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

Gegenstand und Ziele

Im Rahmen laufender Forschungs- und Beratungsarbeit entdeckt SBA Research häufig Schwachstellen in Produkten von Drittanbietern. In unserem Bestreben, die Sicherheit des digitalen Ökosystems zu verbessern, werden ausführliche Sicherheitshinweise gemäß unserer Richtlinie zur Offenlegung von Sicherheitslücken veröffentlichen. Um diese Sicherheitsmeldungen auch zügig melden und bearbeiten zu können, ist SBA Research eine offizielle CVE Numbering Authoritie (CNAs).

Beschreibung des Status

https://www.sba-research.org/sba-security-advisories/

Organisationsfeld

SBA Research

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Kleine und mittlere Unternehmen (KMU)
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Forschung & Entwicklung
- Widerstandsfähigkeit
- Cyberverteidigung

Projekt: FH OÖ F&E GmbH – Cybersecurity Forschung

Start: 1.10.2009
Ende: 31.12.2099
Nr.: 9179

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- 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
- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

Die Research Group des „Department Sichere Informationssysteme“ an der FH Hagenberg verfügt über 15-jährige Erfahrung im Bereich der Auftragsforschung im Cybersecurity-Bereich für die Industrie und Organisationen und hat auch eine langjährige Erfahrung in der Abwicklung von FFG Projekten als Konsortiallead. Die Kombination mit den drei Studiengängen des FH OÖ Departments Sichere Informationssysteme können Synergieeffekte zwischen Forschung und heranwachsenden Expert*innen für Informationssicherheit aus:

- Vollzeit-Bachelorstudium „Sichere Informationssysteme“
- Vollzeit-Masterstudium „Sichere Informationssysteme“
- Berufsbegleitendes Masterstudium „Information Security Management“ intensiv genutzt werden.

Seit der Gründung der Research Group im Jahre 2009 wurden F&E Projekte mit einem Gesamtvolumen von ca. EUR 4 Mio abgewickelt und über 100 Studierende/F&E-Mitarbeiterinnen beschäftigt.

Beschreibung des Status

- 2000 Gründung „Departments für Informationssicherheit“, Start Diplomstudium „Computer- und Mediensicherheit CMS“
- 2009 Einrichtung der Forschungsgruppe

ab 2010 laufender F&E Projektbetrieb, wie z. B. KIRAS Projekte „Cuteforce Analyzer“ und „Realtime Analyzer“. diverse WFE Projekt mit BMLV, Industrieprojekte, …

Organisationsfeld

FH OÖ F&E GmbH, Hagenberg, Department für Informationssicherheit

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Bildung
- Forschung & Entwicklung

Projekt: FH JOANNEUM – Go Cloud Go Secure

Start: 1.11.2024
Ende: 30.10.2026
Nr.: 9180

Aktuelles Jahr
Status: grün
Fortschritt: 10 %

Beschreibung des Status

Im November 2024 gestartet, erste Umsetzung von Arbeitspaketen

Zugrundeliegende Strategische Ziele

- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen
- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Organisationsfeld

FH JOANNEUM Institut Software Design & Security

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Gegenstand und Ziele

EU Erasmus+: Go Cloud Go Secure (KA220-VET) ist ein europäisches Erasmus-Projekt, das Unternehmen, insbesondere KMUs, dabei hilft, Cloud basierende Akititäten sicher zu gestalten. Ergebnisse: Cloud Security Implementation Matrix/Model/Course

Zielgruppe & Themenbereiche

- Bildung
- Forschung & Entwicklung
- Kleine und mittlere Unternehmen (KMU)

Projekt: FH JOANNEUM – RADIUS

Start: 1.1.2025
Ende: 31.12.2029
Nr.: 9181

Aktuelles Jahr
Status: grün
Fortschritt: 5 %

Zugrundeliegende Strategische Ziele

- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit
- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

FFG FH – Forschung für die Wirtschaft 2024 – Research in Artificial Intelligence for Development, Innovation and Upgraded Security ist ein Projekt mit dem Ziel künstliche Intelligenz für die Bereiche Software-Entwicklung, Security industrielle einsetzbar zu machen.

Beschreibung des Status

Im Jänner 2025 gestartet, erste Sondierungstätigkeiten

Organisationsfeld

FH JOANNEUM Institut Software Design & Security

Herausforderungen

Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Forschung & Entwicklung

Projekt: OeNB, FMA – TIBER-AT Implementation

Start: 1.8.2024
Ende: 30.9.2025
Nr.: 9186

Aktuelles Jahr
Status: grün
Fortschritt: 85 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Gegenstand und Ziele

Aufgrund der weltweit steigenden Cyberrisken, des angekündigten Interesses von Marktteilnehmern u. der mit dem Digital Operational Resiliance Act eingeführten Verpflichtung zur Durchführung von europaweit vergleichbaren bedrohungsorientierten Penetrationstests (TLPT – siehe auch Aktivität 8148) für bestimmte Finanzunternehmen haben die Finanzmarktaufsicht (FMA) und die Oesterreichische Nationalbank (OeNB) gemeinsam ein Framework für derartige Tests implementiert. Die Anforderungen von DORA berücksichtigen dabei das bereits etablierte Threat Intelligence-Based Ethical Red Teaming Rahmenwerk (TIBER-EU) des ESZB , das die Vergleichbarkeit der durchgeführten TLPT gewährleisten soll. Die von der FMA und OeNB im November 2023 publizierte und seither angewendete Implementierung von TIBER-EU in Österreich (TIBER-AT) wird nun an die neue Fassung des TIBER-EU Frameworks und die Anforderungen des technischen Regulierungsstandards (RTS) zu TLPT angepasst, das im Laufe des ersten Halbjahres 2025 veröffentlicht wird.

Beschreibung des Status

- Anpassung an aktualisiertes TIBER-EU-Framework
- Anpassung an RTS on TLPT-Anforderungen

Organisationsfeld

OeNB, FMA

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Betreiber wesentlicher Dienste und kritischer Infrastrukturen

Projekt: AIT – KI-basierte Technologien für effektive Cyber Security Schutzmaßnahmen

Start: 1.1.2024
Ende: 31.12.2026
Nr.: 9187

Aktuelles Jahr
Status: grün
Fortschritt: 60 %

Beschreibung des Status

Entwicklung von Lösungen im Zuge von EU Projekten erste Anwendungen

Zugrundeliegende Strategische Ziele

- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen

Gegenstand und Ziele

Entwicklung von Kompetenzen und KI-basierten Technologien für effektive Cyber Security Schutzmaßnahmen

Organisationsfeld

AIT

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Forschung & Entwicklung

Projekt: AIT/GAIA-X – wiki.ATLAWS.eu

Start: 1.1.2024
Ende: 31.12.2026
Nr.: 9188

Aktuelles Jahr
Status: grün
Fortschritt: 80 %

Zugrundeliegende Strategische Ziele

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

Gegenstand und Ziele

Wiki zur Erläuterung der diversen Cyber Security Gesetze – österreichische Open Source Initiative

Beschreibung des Status

Die erste Version wurde am 27.2.2025 in einer Pressekonferenz gelauncht.

Organisationsfeld

AIT/Gaia-X

Herausforderungen

Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Bewusstseinsbildung (Awareness)

Projekt: AIT – Internationales Digital Security Forum (IDSF)

Start: 1.1.2023
Ende: 31.12.2027
Nr.: 9189

Aktuelles Jahr
Status: grün
Fortschritt: 80 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- 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
- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit

Gegenstand und Ziele

Einführung und Etablierung einer internationalen Cyber Security Konferenz in Wien

Beschreibung des Status

Eingeführt und 4. Auflage im Juni 2025 geplant: www.idsf.io

Organisationsfeld

AIT

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Bewusstseinsbildung (Awareness)
- Kleine und mittlere Unternehmen (KMU)
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Forschung & Entwicklung

Projekt: AIT/KSÖ – nationales Cyber Security Planspiel mit Behörden und KRITIS

Start: 1.1.2023
Ende: 31.12.2027
Nr.: 9190

Aktuelles Jahr
Status: grün
Fortschritt: 80 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- 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
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Gegenstand und Ziele

Einführung und Etablierung einer nationalen Cyber Security Übung auf modernsten Simulationsumgebungen

Beschreibung des Status

Regelmäßige nationale Cyber Security Übungen in Österreich etabliert: https://kompetenzzentrum-sicheres-oesterreich.at/2024/11/07/ksoe-ait-und-bawag-veranstalteten-cybersicherheitstraining-fuer-oesterreichische-und-internationale-stakeholder/

Organisationsfeld

AIT/KSÖ

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Kleine und mittlere Unternehmen (KMU)
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Cyberverteidigung
- Widerstandsfähigkeit

Projekt: A1 Seniorenakademie in A1 Shops

Start: 1.1.2023
Ende: 31.12.2099
Nr.: 7150

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

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

Gegenstand und Ziele

A1 bietet in ausgewählten A1 Shops in Wien, Linz, Salzburg, Graz, St. Pölten und Innsbruck wöchentlich kostenlose Schulungen für die Generation 60+ statt. A1 GURUS informieren zu Tipps&Tricks für die optimale und sichere Nutzung des Smartphones.

Beschreibung des Status

Die ausgewählten A1 Shops finden sich auf https://A1Seniorenakademie.at/.

Organisationsfeld

A1 Telekom Austria AG

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Bewusstseinsbildung (Awareness)
- Vertrauen und Privatsphäre

Projekt: A1 digital.campus

Start: 1.1.2020
Ende: 31.12.2099
Nr.: 2067

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

Der A1 digital.campus bietet in Kooperation mit dem Bildungs-Unternehmen DaVinciLab ein vielfältiges kostenloses und innovatives Workshop-Programm an: Kinder und Jugendliche sollen die Scheu vor Technik verlieren und haben die Möglichkeit in die Welt von „Coding“, „Robotik“ und „Media & Design“ einzutauchen und mitzugestalten. Die Kurse finden sowohl am A1 digital.campus oder online, als auch an zahlreichen Schulen in ganz Österreich statt. Zusätzlich arbeiten wir ebenfalls mit Saferinternet zusammen. Die Schwerpunkte sind Studien, Informationsmaterialien, Konzepte, Begutachtung und Beratung in den Bereichen sichere Internet- und Handynutzung und E-Learning. Diese Zusammenarbeit besteht aus der Abhaltung von Workshops für Pädagoginnen (Elementar & Schulpädagoginnen) als auch Informationsabende für Eltern.

Die Pädagoginnen Workshops werden in Zusammenarbeit von Saferinternet und der pädagogischen Hochschule Wien abgehalten.

Beschreibung des Status

Das aktuelle Programm ist abrufbar über die Seite: https://A1digitalcampus.at/

Der Fortschritt wird über die Zahl der tatsächlichen Teilnehmer im Vergleich zum gesteckten Ziel gemessen.

Organisationsfeld

A1 Telekom Austria AG

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

Bildung

Projekt: A1 digital.campus – MINT & Engineering Fokus

Start: 19.2.2024
Ende: 31.12.2099
Nr.: 7148

Aktuelles Jahr
Status: grün
Fortschritt: 10 %

Zugrundeliegende Strategische Ziele

– Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

Der A1 digital.campus bietet ein vielfältiges kostenloses und innovatives Workshop-Programm an: Kinder und Jugendliche sollen die Scheu vor Technik verlieren und haben die Möglichkeit in die Welt von „Coding", „Robotik" und „Media & Design" einzutauchen und dabei selbst viel ausprobieren und zu experimentieren. Zusätzlich veranstalten wir Weiterbildungskurse für Eltern und Pädagog:innen. Die Kurse finden sowohl am A1 digital.campus oder online bzw. on demand statt, als auch an zahlreichen Schulen in ganz Österreich. Unser neuer Kooperationspartner ist Engineering4Kids, die Zusammenarbeit mit Saferinternet, Acodemy und einigen weiteren, neuen Instituten markiert auch eine neue Ausrichtung des Campus ab 2024 auf das MINT und Ingenieurswissenschaft zusätzlich zu den altbewährten Themen von Coding, Robotics und Medienbildung. Detaillierte Informationen zu aktuellen Workshops findet man auf www.a1digitalcampus.at

Beschreibung des Status

Das aktuelle Programm ist abrufbar über die Seite: https://A1digitalcampus.at/

Der Fortschritt wird über die Zahl der tatsächlichen Teilnehmer im Vergleich zum gesteckten Ziel gemessen.

Organisationsfeld

A1 Telekom Austria AG

Herausforderungen

– Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
– Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

Bildung

Projekt: Uni Wien – DaTra

Start: 1.12.2022
Ende: 31.1.2024
Nr.: 8159

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

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

Gegenstand und Ziele

DaTra ist ein Web-Plattform, die nach Anmeldung über Social-Media Plattformen Datenspuren im Netz sucht, diese anschaulich aufbereitet darstellt und einfach umzusetzende Anregungen gibt, wie Privatsphäreneinstellungen von diversen Diensten verbessert werden können. Weiters werden auch Hilfestellungen gegeben werden, wie mit unerwünschten Inhalten (z. B. Bildern) umgegangen werden kann.

Beschreibung des Status

Projekt erfolgreich umgesetzt

- Freie Nutzung des DaTra Tools

https://datra.sec.univie.ac.at/

Organisationsfeld

Universität Wien, Fakultät für Informatik, Forschungsgruppe Security & Privacy

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

Bewusstseinsbildung (Awareness)

Projekt: SBA – ASOC

Start: 1.1.2024
Ende: 1.1.2026
Nr.: 8160

Aktuelles Jahr
Status: grün
Fortschritt: 30 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- 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

Gegenstand und Ziele

Das Forschungsprojekt ASOC hat zum Ziel, einen schnellen und automatisierten Informationsaustausch von Sicherheitsinformationen, IOCs, Regeln, SOAR-Workflows, Use Cases, Playbooks und Wissen im akademischen Kontext zu erforschen. Dieser gemeinsame Ansatz unterstützt die österreichischen Universitäten bei der Aufgabe, ihre digitale Infrastruktur zu schützen, Synergieeffekte optimal zu nutzen und die Cybersicherheit deutlich zu erhöhen, indem proaktive Maßnahmen, Angriffserkennung und Gegenmaßnahmen für alle Beteiligten entwickelt werden.

Beschreibung des Status

https://www.sba-research.org/research/projects/asoc/

Organisationsfeld

SBA Research

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Bildung
- Cyberverteidigung

Projekt: FMA,OENB – TIBER AT Framework

Start: 6.4.2021
Ende: 31.12.2023
Nr.: 2070

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Gegenstand und Ziele

Aufgrund der weltweit steigenden Cyberrisken, des angekündigten Interesses von Marktteilnehmern und der mit dem Digital Operational Resiliance Act (DORA) bevorstehenden Verpflichtung zur Durchführung von europaweit vergleichbaren Threat-led Penetration Tests (TLPT) für ausgewählte Institute, beschließen die Finanzmarktaufsicht (FMA) und die Oesterreichische Nationalbank (OeNB) gemeinsam ein Framework für derartige Tests. Die Anforderungen von DORA (Beschlussfassung bis Ende 2022 zu erwarten) berücksichtigen dabei das bereits in einigen Mitgliedsstaaten etablierte Threat Intelligence-Based Ethical Red-teaming (TIBER) Framework der EZB, welches die Vergleichbarkeit der durchgeführten TLPT gewährleisten soll. Die FMA und OeNB evaluieren daher aktuell eine gemeinsame Implementierung von TIBER in Österreich („TIBER-AT“).

Beschreibung des Status

- Evaluierung und Ausarbeitung eines Konzepts für die Implementierung von TIBER in Österreich
- Planung des Projekts
- Vorbereitungen für eine etwaige Kontaktaufnahme mit EZB TIBER Knowledge Center

Organisationsfeld

FMA. OeNB

Herausforderungen

- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Betreiber wesentlicher Dienste und kritischer Infrastrukturen

Projekt: FMA, OeNB – Threat Led Penetration Testing

Start: 1.1.2023
Ende: 31.12.2099
Nr.: 8148

Aktuelles Jahr
Status: grün
Fortschritt: 85 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Gegenstand und Ziele

Der Digital Operational Resilience Act (DORA) verpflichtet bestimmte Finanzunternehmen ab 2025 zur Durchführung von bedrohungsorientierten Penetrationstests (TLPT – Threat-Led Penetration Testing, siehe auch Aktivität 2070), wobei das Rahmenwerk TIBER-EU des ESZB (siehe auch Aktivität 2070) den relevanten Standard vorgibt. TIBER steht dabei für Threat Intelligence Based Red Teaming. In Vorbereitung auf DORA haben die OeNB und die FMA gemeinsam die Eckpunkte für die Durchführung derartiger Tests in Österreich entwickelt (TIBER-AT). Im Jahr 2024 begann die Pilotphase. Ab 2025 werden gemäß DORA bestimmte Finanzunternehmen in Begleitung des TIBER Cyber Teams Austria (TCT-AT) der OeNB und der FMA verpflichtend TLPT durchführen. Die Durchführung konkreter TLPT gemäß DORA kann unmittelbar nach Inkrafttreten des technischen Regulierungsstandards (RTS) zu TLPT erfolgen.

Beschreibung des Status

- Abschluss der Pilotphase für TIBER-AT aus 2024 in Vorbereitung auf TLPT unter DORA
- Ab 2025: Tourliche Durchführung von TLPT durch Finanzunternehmen gemäß DORA §26-27 nach Inkrafttreten des technischen Regulierungsstandards (RTS) zu TLPT.

Organisationsfeld

FMA, OeNB

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Betreiber wesentlicher Dienste und kritischer Infrastrukturen

Projekt: KSÖ – Baseline Cybersecurity Standard für KMUs

Start: 27.1.2021
Ende: 31.3.2023
Nr.: 1058

Aktuelles Jahr
Status: grün
Fortschritt: 60 %

Zugrundeliegende Strategische Ziele

- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;
- Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten
- 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
- 12 Österreich arbeitet in einem gesamtstaatlichen Ansatz stetig an der Weiterentwicklung seiner Rechtsgrundlagen zur Erhöhung der Cybersicherheit und Bekämpfung der Cyberkriminalität;
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen

Gegenstand und Ziele

Während große Unternehmen und Betreiber kritischer Infrastrukturen bereits seit längerem an ihrer Cyberresilienz arbeiten und zu einem großen Teil bereits über angemessene Sicherheitsstandards verfügen, gibt es insbesondere bei den KMU, welche das Rückgrat der österreichischen Wirtschaft bilden, nach wie vor Nachholbedarf. Um gerade dieser Zielgruppe einen niedrigschwelligen aber dennoch zielführenden Ansatz zur Verfügung zustellen, ihre Basissicherheit aufzubauen, entwickelt der KSÖ gemeinsam mit Cyber Risk Advisory Board, das sich aus Fachexperten der Privatindustrie und der öffentlichen Verwaltung zusammensetzt, das Cyber Risk Rating Schema, welches genau diese Cyber-Basishygiene adressiert. In Zusammenarbeit mit der zuständigen NIS-Behörde soll dieses Schema so weiterentwickelt werden, dass es sich für die voraussichtlich geforderten „Guidelines for SMEs and specifications of their cybersecurity requirements“ als nationale Policy eignet.

Beschreibung des Status

Eine erste Version des Schemas ist vorhanden und wird jährlich weiterentwickelt. Sobald die Anforderungen von NIS 2 vorliegen, soll das Schema in diese Richtung weiterentwickelt werden, dass es von der NIS Behörde als geeignete KMU Policy im Sinne der NIS 2 Anforderungen akzeptiert und mitgetragen wird.

Organisationsfeld

Kompetenzzentrum Sicheres Österreich

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Kleine und mittlere Unternehmen (KMU)
- Wirtschaftsstandort

Projekt: FH OÖ – Fachhochschulausbildung in Informationssicherheit

Start: 31.8.2000
Ende: 31.12.2099
Nr.: 2059

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- 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
- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit

Gegenstand und Ziele

Das „Department Sichere Informationssysteme“ an der FH Hagenberg bildet in drei Ausbildungsschienen Expert*innen für Informationssicherheit aus:

- Vollzeit-Bachelorstudium „Sichere Informationssysteme“
- Vollzeit-Masterstudium „Sichere Informationssysteme“
- Berufsbegleitendes Masterstudium „Information Security Management“

Seit der Gründung im Jahre 2000 wurden bereits mehr als 900 Absolvent*innen als Expert*innen für IT-Security und Informationssicherheit dem europäischen Cyber-Security-Markt zugeführt.

Von 2007 – 2017 wurden in Zusammenarbeit mit dem BMLVS im Rahmen des akademischen Lehrgangs „Akademisch geprüfter Sicherheitsexperte für Informations- und Kommunikationssicherheit – ASICT“ zahlreiche Expert*innen für Informationssicherheit ausgebildet.

Beschreibung des Status

- 2000 Gründung „Departments für Informationssicherheit“, Start Diplomstudium „Computer- und Mediensicherheit CMS“
- 2002 Umwandlung Diplomstudium in Bachelorstudium mit konsekutivem Masterstudium
- 2004 Start Masterstudium „Secure Information Systems“
- 2007 Start akad. LG „Akademisch gepr. SihExp für Informations- und Kommunikationstechnik ASICT“
- 2008 Neukonzeption Vollzeit-Bachelorstudium als „Sichere Informationssysteme BAC SIB“
- 2010 Neukonzeption Vollzeit-Masterstudium als „Sichere Informationssysteme Master SIM“
- 2015 Start berufsbegleitendes Masterstudiums „Information Security Management ISM“
- 2020 Anpassung Vollzeit-BAC-Studium an neue Cyber-Security-Herausforderungen
- 2023 Anpassung Vollzeit-Masterstudium an neue Themen (z. B. KI)

Organisationsfeld

FH Hagenberg, Department für Informationssicherheit

Herausforderungen

- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Bewusstseinsbildung (Awareness)
- Wirtschaftsstandort
- Bildung

Projekt: WKÖ – IT-SAFE

Start: 1.1.2022
Ende: 31.12.2099
Nr.: 2060

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- In Österreich ist eine sichere Partizipation am gesellschaftlichen und politischen Leben im Cyberraum für Bürgerinnen und Bürger möglich
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- 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
- Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen

Gegenstand und Ziele

Ziel von it-safe ist Förderung der Informationssicherheit von Unternehmen, insbesondere KMU. www.it-safe.at ist die Landingpage für cybersicherheitsrelevante Themen für österreichische Unternehmen und bietet kostenlos Webinare, Online-Ratgeber, Checklisten, Informationen zu Förderungen, Suche nach IT-Security-Expert:innen und vieles mehr zum Thema.

Beschreibung des Status

Informationen werden laufend aktualisiert

Organisationsfeld

Wirtschaftskammer Österreich/Bundessparte Information und Consulting

Herausforderungen

- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Kleine und mittlere Unternehmen (KMU)
- Wirtschaftsstandort
- Bewusstseinsbildung (Awareness)

Projekt: WKÖ – CYBER SECURITY HOTLINE WKO

Start: 1.1.2022
Ende: 31.12.2099
Nr.: 2061

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- 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
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen

Gegenstand und Ziele

Die Cyber Security Hotline (cys.at) ist ein bundesweites Gemeinschaftsprojekt der Wirtschaftskammern. Den Mitgliedsbetrieben steht unter 0800 888 133 eine 24/7-Hotline für telefonische Erstinformationen zur Verfügung. Kann nicht bereits hier geholfen werden, wird ein Kontakt zu qualifizierten Mitgliedsbetrieben der Experts Group IT-Security des Fachverbandes Unternehmensberatung, Buchhaltung und IT der WKO (UBIT)hergestellt. Diese haben sich bereit erklärt, im Sinne einer nationalen Sicherheitsstrategie, für kostenfreie telefonische Erstgespräche zur Verfügung zu stehen und mussten eine eigene Zertifizierung der UBIT-Akademie incite bestehen. Sind Sofortmaßnahmen, beispielsweise als Vor-Ort-Einsatz, notwendig, so können diese Leistungen separat mit dem Spezialisten vereinbart werden.

Beschreibung des Status

- Koordination über die Fachgruppen der Unternehmensberatungs-, Buchhaltungsberufe und Informationsdienstleister eingeführt
- Zertifizierung der Spezialisten hinter der technischen Beratung eingeführt und umgesetzt
- Bewerbungsmaßnahmen laufend

Organisationsfeld

Wirtschaftskammern

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Kleine und mittlere Unternehmen (KMU)
- Wirtschaftsstandort

Projekt: WKÖ – CYBER SECURITY FEUERWEHR WKO

Start: 1.1.2022
Ende: 31.12.2099
Nr.: 2062

Aktuelles Jahr
Status: gelb
Fortschritt: 20 %

Zugrundeliegende Strategische Ziele

- In Österreich ist eine sichere Partizipation am gesellschaftlichen und politischen Leben im Cyberraum für Bürgerinnen und Bürger möglich
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen

Gegenstand und Ziele

Erweiterung der CYBER SECURITY HOTLINE WKO um vernetzte Spezialisten im Umfeld der Cyber Security, um eine hollistische und flächendeckende Hilfestellung bei großflächigen Angriffen/Bedrohungen aus dem Cyberraum sicher zu stellen.

Beschreibung des Status

Für die Zukunft wird an dem Ausbau und einem Monitoring-System gearbeitet, da jeder Anruf wie eine Bodenerschütterung zu verstehen ist, die seismische Wellen aufkommender Cyber-Bedrohungen darstellen. Unser Ziel ist ein automatisiertes Frühwarnsystem das, eingebettet in die nationalen Lagebilder, erstmals verkürzte Reaktionsmaßnahmen auf Bedrohungen sicherstellt.

Organisationsfeld

Wirtschaftskammer STMK

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

- Forschung & Entwicklung
- Wirtschaftsstandort
- Kleine und mittlere Unternehmen (KMU)
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Widerstandsfähigkeit
- Cyberkriminalität und Strafverfolgung
- Cyberverteidigung

Projekt: WKÖ – Women4Cyber Austria

Start: 31.8.2022
Ende: 31.12.2099
Nr.: 8161

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- 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
- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen
- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren

Gegenstand und Ziele

Women4CyberAustria das öst. Chapter der eurpäischen NPO Women4Cyber, deren Ziel es ist Frauen im Bereich der Cybersicherheit zu fördern, zu ermutigen und zu unterstützen und das Bewusstsein für eine gender-inklusive Cybersicherheits-Community zu erhöhen.

Beschreibung des Status

fortlaufende Aktivitäten

Organisationsfeld

Women4Cyber Austria

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Bildung
- Bewusstseinsbildung (Awareness)

Projekt: VERBUND – OT Cyber Security Lab

Start: 14.6.2020
Ende: 31.12.2023
Nr.: 2063

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Gegenstand und Ziele

Das OT Cyber Security Lab wurde 2020 gegründet und wird seither aufgebaut. Den zentralen Angelpunkt stellt eine Testumgebung dar, in der neue Systeme der OT (Operational Technology) bereitgestellt u. Prozesse aus dem Kraftwerksbetrieb realitätsnah abgebildet werden. Die Systeme werden anschließend Cyber Security Prüfungen (Penetration Tests) unterzogen u. gemeinsam mit externen Partnern u. Forschungseinrichtungen werden neue Methoden zur Absicherung der OT Infrastruktur entwickelt u. getestet. In die Projekte und die laufende Arbeit des OT Cyber Security Lab werden sowohl Partner aus der Industrie (Anlagenhersteller, OT-Anbieter, Anbieter von Security-Lösungen) einbezogen als auch Organisationen aus Forschung und Entwicklung (Unis, FH, Forschungsinstitute). Ergebnisse aus dem Lab werden auch publiziert und somit teilweise der Öffentlichkeit zur Verfügung gestellt. In letzter Zeit wurde darüber hinaus ein Schwerpunkt Frauenförderung umgesetzt, um Schülerinnen und Studentin IT- und OT-Security näher zu bringen.

Beschreibung des Status

Das Projekt wurde Ende 2023 abgeschlossen. Seit 2024 wird das OT Cyber Security Lab regulär als Teil der Abteilung Informationssicherheit von VERBUND weitergeführt. Es werden laufend neue Projekte aufgesetzt. Wir freuen uns über Interessent:innen und neue Kooperationspartner.

Organisationsfeld

VERBUND AG, Abteilung Informationssicherheit

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Forschung & Entwicklung
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Wirtschaftsstandort

Projekt: COMPARO – OPSAM Community Edition: zentrale Wissensdrehscheibe Cybersicherheit

Start: 30.9.2021
Ende: 31.12.2025
Nr.: 2064

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- 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
- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit
- Österreich arbeitet in einem gesamtstaatlichen Ansatz stetig an der Weiterentwicklung seiner Rechtsgrundlagen zur Erhöhung der Cybersicherheit und Bekämpfung der Cyberkriminalität;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen

Gegenstand und Ziele

In der OPSAM Community Edition werden Informationen und Hilfsmittel zur Cybersicherheit von Organisationen, Unternehmen und Websites zur Verfügung gestellt.

- Besonderen Wert legen wir in der aktuellen Weiterentwicklung auf frei verfügbare Informationen von öffentlichen Einrichtungen oder Organisationen (z. B. BKA, BSI, ENISA usw.)
- Diese werden durch OPSAM auffindbar, transparent und zeigen konkrete Lösungsansätze.
- Die bereits realisierte OPSAM Communityedition macht vorhandene Wissens- bzw. Lösungsbausteine verfügbar und hilft Unternehmen aller Größenordnungen effektiv ihre Cybersicherheit zu erhöhen.
- Gemeinsam mit bestehenden Einrichtungen und Organisationen wird diese als zentrale Wissensdrehscheibe für Österreich verfügbar und weiterentwickelt.
- Sie ermöglicht Ein- und Überblick zu Normen, Standards, Handlungsfeldern und Lösungsansätzen im Cybersicherheitsmanagement, einfache Suchmechanismen und Referenzierung relevanter Informationsquellen

https://comparo.eu/cca

Beschreibung des Status

- Fachliche Recherche mit Anwender*innen in der D-A-CH Region (VOICE-CIO Community) von 01/2019 bis 12/2020
- Wöchentliche Bewertung aktueller Bedrohungslagen und Lösungsansätze von 01/2020 bis 12/2021
- Wöchentliche Meilensteine zur Entwicklung und Design von Lösungsbausteinen in der D-A-CH Region
- Sammlung und Aufbau von Wissensbausteinen für öffentlich verfügbar und somit referenzierbarer Informationen und Hilfsmittel
- Laufende Aktualisierung
- Entwicklung des Grundmodells
- Prototypisierung in Technologieumgebungen bis 07/2021
- Verfügbarkeit der Version 1.0 in 12/2021
- Laufender Ausbau und Erweiterung seit 01/2022

Organisationsfeld

Comparo

Herausforderungen

- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Internationale Zusammenarbeit
- Widerstandsfähigkeit
- Forschung & Entwicklung
- Bildung
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Wirtschaftsstandort
- Bewusstseinsbildung (Awareness)
- Vertrauen und Privatsphäre
- Kleine und mittlere Unternehmen (KMU)

Projekt: DVC – Trainingskurs OPCYBRES: Cybersicherheit als Eckpfeiler der Unternehmensresilienz

Start: 1.11.2021
Ende: 31.12.2099
Nr.: 2065

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit
- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- In Österreich ist eine sichere Partizipation am gesellschaftlichen und politischen Leben im Cyberraum für Bürgerinnen und Bürger möglich
- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Gegenstand und Ziele

Der frei verfügbare Trainingskurs OPCYBRES steht für Operative Power für Cyber Resiliente Unternehmen. Resilienz im Cyber Space ist gerade für Klein- und mittelständische Unternehmen eine Herausforderung mit oftmals unterschätzter Komplexität. Sie entsteht durch Abhängigkeiten von kleinteiligen Softwaretools, Prozessen, Methoden und die Abhängigkeit von den eigenen und den Fähigkeiten dritter, um die Auswirkungen der Software, ihrer Anwendung und ihrer Risiken einschätzen zu können.

- Teil 1: Einführung in System der Komplexität/Systemdenken, Vorstellung der 7 Kernbereiche für umfassende Cybersicherheitsstrategie
- Teil 2: Anwendung von Security-by-Design: Auswirkungen ganzheitlichen Cybersicherheitsanspruches auf Produkte, Services, Ökosysteme und operative Abläufe; Schärfung Resilienzsensing
- In Teil 3: Einführung in Ereignis- & Angriffsanalyse sowie Bewertung auf Basis des 4-Quadrantenmodells und umfassende Bedrohungsanalyse; Umgang mit der OPSAM Communityedition von Comparo und digital value creators

Beschreibung des Status

OPCYBRES ist seit Januar 2023 verfügbar und wird bereits von Kursteilnehmenden genutzt und angewendet. Das Angebot wird zukünftig – sobald der Knowhow Buddy fertiggestellt ist – direkt auf www.barbara-fluegge.com verfügbar sein in einem eigenen Lern/Erfahrung-Bereich. Der OPCYBRES© Basis-Kurs bleibt kostenfrei verfügbar für alle.

Organisationsfeld

digital value creators (DVC) Consulting

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Vertrauen und Privatsphäre
- Bewusstseinsbildung (Awareness)
- Wirtschaftsstandort
- Forschung & Entwicklung
- Widerstandsfähigkeit

Projekt: KPMG/KSÖ-Cybersicherheitsstudie „Cybersecurity in Österreich”

Start: 1.8.2024
Ende: 30.6.2025
Nr.: 2071

Aktuelles Jahr
Status: grün
Fortschritt: 20 %

Zugrundeliegende Strategische Ziele

- 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
- In Österreich ist eine sichere Partizipation am gesellschaftlichen und politischen Leben im Cyberraum für Bürgerinnen und Bürger möglich
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

Die KPMG veröffentlicht jährlich in Zusammenarbeit mit dem Sicherheitsforum Digitale Wirtschaft des Kompetenzzentrums Sicheres Österreich (KSÖ) die Cyber Security Studie für Österreich. Die neunte Auflage der Studie in Folge, an der 2024 1.158 Unternehmen aus Österreich teilgenommen haben, ist ein Gradmesser für die Sicherheitslage und das Stimmungsbild heimischer Unternehmen und der öffentlichen Verwaltung in Sachen Cybersecurity. Ergänzt wird diese Studie Jährlich mit Experteninterviews sowie einem Round-Table, an dem Vertreter unterschiedlicher Institutionen und Unternehmen aus dem In- und Ausland teilnehmen. Diese Interviewpartner bestätigen einerseits die Zahlen aus der Studie und die aktuellen Trends oder ergänzen die Studie jährlich um neue Sichtweisen, Facetten und Aspekte, an die bis dato vielleicht noch nicht gedacht wurde. Darüber hinaus sollen aktuelle Trends und Entwicklungen aufgezeigt werden und zur Sensibilisierung der Gesellschaft im Umgang mit digitalen Informationen beigetragen werden.

Beschreibung des Status

Die 9. Ausgabe der Cyber Security Studie für das Jahr 2024 abgeschlossen und wurde im April 2024 beim ÖAMTC der Öffentlichkeit Die Planungen und Aufbereitungen der Inhalte für die 10. Ausgabe laufen bereits. Diese soll voraussichtlich im Mai 2025 veröffentlicht und präsentiert.

Organisationsfeld

KPMG Security Services GmbH

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Cyberkriminalität und Strafverfolgung
- Widerstandsfähigkeit
- Forschung & Entwicklung
- Kleine und mittlere Unternehmen (KMU)
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Wirtschaftsstandort
- Bewusstseinsbildung (Awareness)
- Vertrauen und Privatsphäre

Projekt: KPMG – Cyber Awareness Monat Oktober 2024: Sensibilisierung und Trainings

Start: 31.5.2024
Ende: 31.12.2024
Nr.: 7149

Aktuelles Jahr
Status: grün
Fortschritt: 40 %

Zugrundeliegende Strategische Ziele

- In Österreich ist eine sichere Partizipation am gesellschaftlichen und politischen Leben im Cyberraum für Bürgerinnen und Bürger möglich
- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

Die zunehmende Vernetzung in der digitalen Welt und die intensive Nutzung von digitalen Kommunikationskanälen führt dazu, dass Jugendliche vor immer größeren Herausforderungen im Umgang mit diesen Technologien stehen. Neben den Funktionen spielt vor allem die Sicherheit eine immer größere Rolle, um die eigene Identität zu schützen. In diesem Zusammenhang führt KPMG (KPMG Security Services GmbH) jährlich an Schulen in Österreich (NMS, AHS, BG/BRG, BORG, BHS) jährlich kostenlose Awareness Trainings an heimischen Schulen durch. Expert:innen von KPMG besuchen die interessierten Schulen und geben den Schüler:innen und Lehrer:innen praxisnahe Einblicke in die aktuellen Herausforderungen und zeigen Möglichkeiten, wie man sich selbst, das eigene Umfeld oder die eigene Familie entsprechend schützen kann.

Die erstellten Unterlagen werden den Schüler:innen und Lehrkräften kostenlos zur Verfügung gestellt und dienen als Impulsgeber für weitere Ausbildungsblöcke zur Stärkung der digitalen Grundbildung und Kompetenzen

Beschreibung des Status

- Planung des Vorhabens abgeschlossen
- Schulen kontaktiert und über das Angebot informiert
- Erste Rückmeldungen sind eingetroffen
- Finale Rückmeldungen bis 15.9.2024
- Planung der Schulbesuche und Trainings ab Anfang Oktober 2024
- Abschluss der Trainings in den Schulen bis 15. November 2024
- Zusammenfassung und Nachbericht

Organisationsfeld

KPMG Security Services GmbH

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Vertrauen und Privatsphäre
- Bewusstseinsbildung (Awareness)
- Freier Meinungsbildungsprozess
- Ethik
- Bildung

Projekt: INDUCE Cyber Security Literacy And Dexterity through Cyber Exercises

Start: 1.4.2021
Ende: 31.3.2024
Nr.: 2072

Aktuelles Jahr
Status: grün
Fortschritt: 30 %

Zugrundeliegende Strategische Ziele

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

Gegenstand und Ziele

INDUCE zielt darauf ab, Cybersicherheitskompetenzen und -fähigkeiten mit Cyber-Übungen für eine breite Zielgruppe zugänglich zu machen. Im Rahmen des Projektes werden daher existierende Cyber-Übungen (z. B. Technologien oder Cyber-Szenarien) anhand der Diversitätsdimensionen und Chancengerechtigkeit evaluiert und aufbauend darauf neu entwickelt, erweitert bzw. adaptiert. Diese Konzepte, Methoden und Werkzeuge für Cyber-Übungen werden in Future Labs gemeinsam mit potentiellen Zielgruppen getestet, um Open Innovation zu unterstützen. Zudem ermöglichen der Aufbau und die Förderung eines interdisziplinären Innovationsnetzwerkes für Wirtschaft, Behörden und Forschung den Wissens- und Technologietransfer. Mit INDUCE können langfristig Cybersicherheitskompetenzen für die Bevölkerung aufgebaut und weiterentwickelt werden, die zur Handlungsfähigkeit vielfältiger Zielgruppen in einer digitalen Gesellschaft beitragen.

Beschreibung des Status

Beginn: April 2021

Dauer: 3 Jahre,

1. Projektjahr: Evaluierung des vorhandenen Angebots an Cyber-Übungen, Diversitätsanalyse, Zielgruppen-Bestimmung, Planung der Umsetzung

Organisationsfeld

Kompetenzzentrum Sicheres Österreich im Konsortium mit: AIT, Fachhochschule Oberösterreich, Infraprotect, CSA

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Vertrauen und Privatsphäre
- Bewusstseinsbildung (Awareness)
- Kleine und mittlere Unternehmen (KMU)

Projekt: AIT – Post-Quanten-Computer sichere Verschlüsselung für höchste Cyber Sicherheit

Start: 1.1.2021
Ende: 31.12.2026
Nr.: 2073

Aktuelles Jahr
Status: grün
Fortschritt: 70 %

Zugrundeliegende Strategische Ziele

- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

(i) Österreich als führendes Kompetenzzentrum global zu etablieren und (ii) als ein wichtiger Technologielieferant in der EU zu positionieren. (iii) Realisierung von effektiven Multi-stakeholder-Umsetzungsinitiativen mit Behörden und (iv) Implementierung einer international führenden Quanten-Computer sicheren Verschlüsselungstechnologieinfrastruktur in der Behördenkommunikation im Kontext von strategischen EU Initiativen wie EuroQCI und IRIS2 (Infrastruktur für Resilienz, Interkonnektivität und Sicherheit durch Satelliten) -https://www.consilium.europa.eu/de/press/press-releases/2022/11/17/council-and-european-parliament-agree-on-boosting-secure-communications-with-a-new-satellite-system/

Beschreibung des Status

Österreich ist durch AIT als einer der führenden Technologieanbieter für die EU Industrie etabliert (ESA, EU-Cyber Security Industrie). Österreich ist durch AIT als führendes Kompetenzzentrum in der EU etabliert; nationale Infrastrukturumsetzungsinitiativen finanziert und gestartet – Digital Europe Programme (DEP), nationales KIRAS Projekt, etc.); Umsetzungsinitiativen für österr. Behörden etabliert. ESA Kooperation etabliert.

Organisationsfeld

AIT

Herausforderungen

Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Internationale Zusammenarbeit
- Widerstandsfähigkeit

Projekt: AIT – Ausbau der Cyber-Security Widerstandsfähigkeit für kritische Infrastrukturbetreiber in AT

Start: 1.1.2021
Ende: 31.12.2026
Nr.: 2074

Aktuelles Jahr
Status: grün
Fortschritt: 95 %

Zugrundeliegende Strategische Ziele

- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- 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

Gegenstand und Ziele

Durchführung von Capability-Development Maßnahmen für kritische Infrastrukturbetreiber und Validierung von effektiven Cyber-Security Prozessen für Infrastrukturbetreiber und Behörden. Verwendung von modernster „made in Austria" Technologien zur Simulation von Cyber-Bedrohungen und Training von Abwehrmaßnahmen. Positionierung Österreichs als einer der global führenden Cyber Range Plattform-Anbieter für kritische Infrastrukturbetreiber.

Beschreibung des Status

(i) International führende Kompetenzen, Methoden und Werkzeuge wurden in Österreich am AIT implementiert. Österr. hat sich als international führendes Kompetenzzentrum im Bereich Cyber Securit etabliert – das AIT ist das erste u. derzeit einzige offizielle „Collaboration Center" der IAEA zum Thema Cyber Security. In dieser Rolle werden Cyber Security Trainings für kritische Infrastrukturbetreiber weltweit durchgeführt

(ii) Aufbau Trainings- und Simulationsplattformen für Cyber Sicherheitstrainings im IT und OT-Bereich (www.cyberrange.at).

(iii) erfolgreiche Erweiterung in andere kritische Infrastrukturbereiche und Positionierung des Standortes Österreich im Kontext der EU Diskussion zum Aufbau einer EU Cyber Security Skill Academy.

Organisationsfeld

AIT

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Kleine und mittlere Unternehmen (KMU)
- Wirtschaftsstandort
- Internationale Zusammenarbeit

Projekt: Learners – effizientere Methodologien + Methodiken komplexe und Dynamische Inhalte für Jugend

Start: 1.4.2022
Ende: 31.12.2023
Nr.: 2078

Aktuelles Jahr
Status: 🟡 gelb
Fortschritt: 4 %

Zugrundeliegende Strategische Ziele

Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

Aufgrund der zunehmenden Komplexität technisch vernetzter Systeme, aber auch der schnelllebigen Änderungen in diesem Bereich, wird die Materie immer unübersichtlicher. Somit wird es zunehmend schwieriger ein vollständiges Bild aller Komponenten im System zu erhalten, was Potenzial für neue Angriffsmuster eröffnet. Die als extrem hoch wahrgenommene Komplexität der Materie hat den Effekt, dass es zunehmend verabsäumt wird Kindern und Jugendlichen aber Erwachsenenden richtigen Umgang mit Onlinemedien zu lernen. Den Großteil ihrer online Kompetenzen trainieren sich diese somit selbst an, was spezielle Aspekte von vornherein außen vorlässt. Basierend auf diesem Umstand, fehlt den Kindern und Jugendlichen das Bewusstsein für Cybersicherheit und ihre Möglichkeiten sich „sicher“ im digitalen Raum zu bewegen. Mangelndes Sicherheitsempfinden und -wissen haben die Ursache, dass Cybersicherheitsvorfälle gehäuft eintreten und immer schwerere Schäden verursachen.

Beschreibung des Status

On Hold – Finanzierungsfrage ungeklärt! Um die skizzierte Problemstellung zu adressieren, zielt das Projekt LEARNERS darauf ab eine innovative Ausbildung im Bereich digitale Kompetenzen und Cybersicherheit an Schulen im Bereich der 10-14-Jährigen zu entwickeln. Die Lehrinhalte sollen sich dabei sowohl an die Lehrenden („train the trainers“) als auch Schüler*innen richten.

Projektpartner: CSA, AIT, SBA, UniWien, FH OÖ

Organisationsfeld

CSA – CyberSecurityAustria

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Bildung

Projekt: Nationales Cyber Security Trainingszentrum

Start: 31.8.2022
Ende: 31.12.2025
Nr.: 2079

Aktuelles Jahr
Status: 🟡 gelb
Fortschritt: 2 %

Zugrundeliegende Strategische Ziele

Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

Effektives Cybersecurity Ausbildungs- und Trainingsprogramm als wichtiger Bestandteil einer nachhaltigen Cybersecurity Schutzstrategie unserer umfassenden Digitalisierung – eine Kooperation von AIT, SBA Research, Uni Wien, TU Wien, ISTA und CSA Austria

Um technische Cybersecurity Schutzmethoden effektiv zu ergänzen und die menschliche Komponente in ein umfassendes Schutzkonzept für digitale Infrastrukturen zu berücksichtigen, sind verschieden Ausbildungs- und Trainingsvorhaben unumgänglich.

Ein Aufbauen auf vorhandenen Kompetenzen und Infrastrukturen im Bereich Cybersecurity in Österreich ist dabei eine wichtige Grundlage für die Sicherstellung entsprechender Synergieeffekte und Erreichung höchster Effektivität.

Beschreibung des Status

On Hold – Finanzierungsfrage ungeklärt!

Projektpartner: CSA, AIT,SBA, TUWien, UniWien

Organisationsfeld

CSA – CyberSecurityAustria

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Bildung

Projekt: VISP – Vienna InternetSecurityPrivacy Cluster

Start: 1.3.2020
Ende: 31.12.2099
Nr.: 2081

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren

Gegenstand und Ziele

ViSP – der Vienna Cybersecurity and Privacy Research Cluster – besteht aus ForscherInnen von AIT Austrian Institute of Technology, CSA Cybersecurity Austria, IST Austria, SBA Research, TU Wien und Uni Wien. Die Mission von ViSP ist es, das wahre Potenzial des Standorts durch die Förderung von Kooperationen zwischen verschiedenen Instituten in Wien zu erschließen. Durch diese Zusammenarbeit streben wir danach, wirkungsvolle Forschung zu betreiben, den Stand der Technik voranzutreiben und exzellente Ausbildung um Wien eine Vorreiterrolle in der Forschung im Bereich Sicherheit und Datenschutz zu sichern.

Beschreibung des Status

- laufende Aktivitäten wie Gastvorträge renumierter Forschenden
- Auflistung aller Security Lehrveranstaltungen auf TU Wien und Uni Wien
- verstärkte Kooperation im Zuge von Forschungsprojekten

https://visp.wien

Organisationsfeld

Universität Wien, TU Wien, IST Austria, SBA Research, AIT Austrian Institut of Technology, CSA Cyber Security Austria

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Bildung

Projekt: OCG – Young Researchers Day

Start: 1.3.2024
Ende: 31.12.2099
Nr.: 8157

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren

Gegenstand und Ziele

Der Young Researchers´ Day wird im Rahmen der IKT-Sicherheitskonferenz des Österreichischen Bundesheeres abgehalten. Dieses Event wird von OCG Arbeitskreis IT-Sicherung und dem FFG COMET Kompetenzzentrum SBA Research organisiert. Jungforschende können im Zuge der IKT ihre Forschung vorstellen. Ziel ist die Cybersecurity-Nachwuchsförderung.

Beschreibung des Status

- Findet jährlich im Zuge der IKT Sicherheitskonferenz statt
- alle Security einschlägigen Universitäten und Fachhochschule werden kontaktiert
- ProfessorInnen nominieren Master- und PhD-Arbeiten für YRD
- Vorträge der wissenschaftlichen Arbeiten bei IKT Sicherheitskonferenz
- Darstellung der Forschungsarbeiten im OCG Journal

Organisationsfeld

OCG Arbeitsgruppe Security

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

Forschung & Entwicklung

Projekt: CSA – HackFu

Start: 30.9.2022
Ende: 29.9.2023
Nr.: 2080

Aktuelles Jahr
Status: grün
Fortschritt: 15 %

Zugrundeliegende Strategische Ziele

Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

HackFu Austria ist ein 3-tägiges Event rund um das Thema Cyber- und IT-Security, das 2020 erstmals in Österreich abgehalten wurde und das eine realistische Bedrohung im Bereich Cyberkriminalität und/oder -terrorismus simuliert. Es richtet sich an (jetzige und zukünftige) Experten aus den fachspezifischen Kreisen, der IT-Security Branche, und FHs und Unis. Neben der Erweiterung der Kompetenzen der Teilnehmenden sind Kooperation, Austausch von Expertise und Know-How, Networking und Teambuilding zentrale Komponenten des Vorhabens. Durch die Zusammenarbeit der 100 besten Köpfe, die Österreich im Bereich der Cyber-Security zu bieten hat, wird ein Austausch und Know-How Transfer ermöglicht, der landesweit einzigartig ist.

Beschreibung des Status

Evaluierungen für 2023 sind angelaufen ! Auf dem dreitägigen Event, das als eine „Gamified Convention“ beschrieben werden kann, kommen rund 100 Talents und Experts aus dem Bereich der Netzwerk- und Informationstechnik zusammen und müssen durch das Lösen verschiedener Aufgaben einen übergeordneten Auftrag erfüllen, nämlich ein Stück der kritischen Infrastruktur „zurückzuhacken“. Die 5 Teams zu je 20 Teilnehmenden müssen ihre Fähigkeiten in den Bereichen team-interne und darüberhinausgehende Kooperation, Expertise und Know-How, Networking und Teamarbeit unter Beweis stellen.

Organisationsfeld

CSA – CyberSecurityAustria

Herausforderungen

- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Bildung

Projekt: „Shecurity“ – Hackerinnen Training

Start: 31.5.2023
Ende: 31.12.2099
Nr.: 8155

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

Das Hackerinnen Training bietet Mädchen, Frauen und FINTA*, die Interesse an IT-Sicherheit haben und mehr über die technische Seite der Security erfahren wollen, monatliche und kostenfreie Trainings an.

Ziel ist es Interesse und Begeisterung wecken, hochwertige Trainings und somit einen einfachen Einstieg in die Security ermöglichen, sowie Fähigkeiten stärken und weiterentwickeln. Es gibt keine Einschränkungen bezüglich Alter oder Vorwissen. Weiters ist ein Einstieg in das Programm jederzeit möglich. Neben den thematischen Trainings, finden regelmäßig Übungen in Kleingruppen und auch Teambuilding Events statt.

Beschreibung des Status

- monatliche Trainings
- kontinuierliche Weiterentwicklung der Trainings
- Community Building

https://verbotengut.at/allgemein/hackerinnen-training/

Organisationsfeld

CSA Cybersecurity Austria, TU Wien Cysec

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

Bildung

Projekt: SBA, sec4dev – youTube Kanal

Start: 4.9.2015
Ende: 31.12.2099
Nr.: 8158

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren

Gegenstand und Ziele

In den Youtube Kanälen SBA Research und sec4dev sind eine große Anzahl an Vortragsvideos zu unterschiedlichen Security Themen zu finden.

Beschreibung des Status

SBA Research

https://www.youtube.com/@SBAResearch-IT-Security

sec4dev

Alles rund um Security in der Softwareentwicklung

https://www.youtube.com/@sec4devconferencebootcamp996

Organisationsfeld

SBA Research

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Bewusstseinsbildung (Awareness)
- Bildung

Projekt: SBA, ÖIAT – Security Awareness Stammtisch

Start: 24.4.2023
Ende: 31.12.2099
Nr.: 8156

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Gegenstand und Ziele

Endbenutzer:innen sind das wichtigste und stärkste Glied der Sicherheitskette. Awareness ist daher wichtigstes Erfolgskriterium für mehr IT-Sicherheit in Unternehmen. In einem informellen und vertrauensvollen Rahmen können Security Awareness Verantwortliche Praxiserfahrungen austauschen und aktuelle Trends und Herausforderungen diskutieren. Das Lernen von- und miteinander steht dabei im Mittelpunkt.

Beschreibung des Status

Laufende Treffen alle zwei bis drei Monate

Organisationsfeld

SBA Research, ÖIAT Österreichisches Institut für angewandte Telekommunikation

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

Bildung

Projekt: SBA – Cybersecurity Quiz

Start: 30.9.2021
Ende: 31.12.2099
Nr.: 8154

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

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

Gegenstand und Ziele

Das Cyber Security Quiz (kostenfrei) bietet einen breiten Überblick über die Herausforderungen, von Schadsoftware über Online-Betrug bis hin zu Datenschutz, Hass im Netz und Algorithmen und Künstliche Intelligenz. In 13 Themen sind die Inhalte kurz, spielerisch & interaktiv aufgearbeitet. Die App kann bereits 21.300 UserInnen aufweisen und wird gerne in Schulen eingesetzt. Weiters hat das Cyber Security Quiz wiederholt das Gütesiegel „Lern App“ des Oead bekommen. Übe für dich alleine oder stürze dich in ein österreichweites Quizduell und werde Cyber Security Master!

Beschreibung des Status

- App ist für die Öffentlichkeit frei verfügbar
- Module werden laufend erweitert
- Ist in den Sprachen Deutsch und Englisch verfügbar

https://cybersecurityquiz.at/

Organisationsfeld

SBA Research, Ovos Play, ÖIAT, CSA Cybersecurity Austria

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Bewusstseinsbildung (Awareness)
- Kleine und mittlere Unternehmen (KMU)
- Bildung

Projekt: SBA – securepizza.club @ SBA Research

Start: 1.1.2021
Ende: 31.12.2099
Nr.: 2082

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;

Gegenstand und Ziele

Der Club soll als Plattform für Studierende und als Treffpunkt dienen. Ein Ort, an dem man sich zu aktuellen Sicherheitsthemen u. a. von (akademischen) Sicherheitskonferenzen austauschen, über neue Sicherheitsthemen sprechen und Ideen austauschen kann. Damit soll das Interesse an Security bei den Studierenden geweckt und verstärkt werden.

Beschreibung des Status

Securepizzaclub findet laufend statt

https://www.sba-research.org/securepizza-club-sba-research/

Organisationsfeld

SBA Research

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

Bildung

Projekt: SBA – Women in Privacy & Security Vienna

Start: 1.1.2021
Ende: 31.12.2099
Nr.: 2083

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;

Gegenstand und Ziele

Wir sind eine in Wien ansässige Community von Studentinnen, jungen Akademikerinnen, Verbündeten und Befürworterinnen, die sich zum Ziel gesetzt hat, talentierte Frauen zusammenzubringen, um ihre Leidenschaft und ihren Einsatz für den Schutz der Privatsphäre und die Sicherheit zu fördern.

Beschreibung des Status

Meetup findet laufend statt

https://www.meetup.com/SecWomenVienna/

Organisationsfeld

SBA Research

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Bewusstseinsbildung (Awareness)
- Bildung

Projekt: SBA – Seurity Meetup

Start: 1.1.2021
Ende: 31.12.2099
Nr.: 2084

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen

Gegenstand und Ziele

Wir beabsichtigen, eine Gemeinschaft von Menschen aufzubauen und zu fördern, die sich für IT- und Informationssicherheit und verwandte Bereiche interessieren. Unsere Mission ist es, die Sicherheit zu einem Bürger erster Klasse in der Welt der Softwareentwicklung zu machen!

Beschreibung des Status

Meetups findet laufend statt

https://www.meetup.com/security-meetup-by-sba-research/

Organisationsfeld

SBA Research

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Bewusstseinsbildung (Awareness)
- Kleine und mittlere Unternehmen (KMU)
- Bildung

Projekt: ISPA – Der Online-Zoo

Start: 1.12.2015
Ende: 1.7.2025
Nr.: 3098

Aktuelles Jahr
Status: grün
Fortschritt: 75 %

Zugrundeliegende Strategische Ziele

- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- In Österreich ist eine sichere Partizipation am gesellschaftlichen und politischen Leben im Cyberraum für Bürgerinnen und Bürger möglich

Gegenstand und Ziele

Das Buch richtet sich an Kinder im Vorschul- und Volksschulalter (4–9 Jahre) und soll diese auf spielerische Art an das Internet heranführen. Ziel ist es, den Kindern erste digitale Kompetenzen zu vermitteln, aber auch bei den Erziehungsberechtigten ein Bewusstsein für die Notwendigkeit früher Medienbildung zu schaffen.

Das Kinderbuch wurde mittlerweile in dreizehn Sprachen übersetzt, zuletzt ins ukrainische, und auch eine Video-Reihe zu einzelnen Geschichten erstellt. Darüber hinaus stellt die ISPA auch ein medienpädagogisches Begleithandbuch für Eltern, Pädagoginnen und Pädagogen sowie andere Bezugspersonen von Kindern und möchte diese dabei unterstützen, gemeinsam mit jungen Menschen Themen wie den richtigen Umgang mit Informationen und Quellen, Selbstbewusstsein in digitalen Kontexten und den verantwortungsvollen Umgang mit eigenen Daten zu erschließen.

Beschreibung des Status

- Projektbeginn 2015
- Erstausgabe 2016
- Veröffentlichung medienpädagogisches Begleithandbuch 2017
- Veröffentlichung Videoreihe 2021
- Übersetzung ins Ukrainische
- Neuauflage 2022
- Veröffentlichung auf www.ispa.at sowie Druckexemplare an Stakeholder
- Verteilung an Schulen und Interessierte auf Anfrage, kostenfrei

Organisationsfeld

ISPA

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Bewusstseinsbildung (Awareness)
- Bildung

Projekt: ACSC – Austrian Cyber Security Challenge 2023

Start: 1.1.2023
Ende: 31.12.2023
Nr.: 4103

Aktuelles Jahr
Status: grün
Fortschritt: 60 %

Zugrundeliegende Strategische Ziele

Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

Die AUSTRIACYBERSECURITYCHALLENGE ist ein seit 2012 jährlich stattfindender Bundesweiter IT-Sicherheits-Talente (Hacker) Wettbewerb der sich direkt an Schüler/Schulen und Studenten/Universitäten und indirekt an alle Stakeholder unserer Gesellschaft richtet. Analog zur Nachwuchsarbeit im Spitzensport sollen dabei nicht nur junge Talente entdeckt, gefordert und gefördert werden sondern neben Ausbildungsstätten und Lehrenden auch breite Teile unserer Gesellschaft für das Thema und die Notwendigkeit CyberSecurity sensibilisiert werden. Der Bewerb dient zudem diese Talente gezielt an die heimischen Unternehmen und Behörden heranzuführen und als Leuchtturmprojekt dem grassierenden Fachkräftemängel im IT(Security) Bereich entgegen zu wirken.

Beschreibung des Status

Die ACSC wird 2023 bereits zum 12 mal durchgeführt. Die Challenge konnte sich als fixe Größe mit über 500 Teilnehmern in den letzten Jahre im heimischen Ausbildungs- und Security-Bereich etablieren. Das AT Modell wurde 2014 von der ENISA als Ausgangsmodell für paneuropäische Spiele herangezogen und wird in allen EU Ländern ausgetragen (siehe ECSC). Auch die offene Klasse österr. Staatsmeisterschaft mit rund 150 Teilnehmern findet Ihren Ursprung in der ACSC sie richtet sich an schon berufstätige Securityspezialisten und dient nicht nur Wettbewerb und Benchmarking sondern vor allem dem Peering und Vertrauensbildung unter den heimischen Sicherheitsspezialisten.

Organisationsfeld

CSA – CyberSecurityAustria

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Bildung

Projekt: ECSC – European Cyber Security Challenge 2023

Start: 1.1.2023
Ende: 31.12.2023
Nr.: 4104

Aktuelles Jahr
Status: grün
Fortschritt: 50 %

Zugrundeliegende Strategische Ziele

Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

Die EuropeanCyberSecurityChallenge ECSC (ecsc,eu) ist die Europameisterschaft der Nachwuchshacker aus 26 Europäischen Nationen. Die Nationalteams, bestehend aus jeweils 10 der besten SchülerInnen und StudentInnen dieser Länder treten gegeneinander in einem Europäischen Finale an, um den Europäischen Champion zu ermitteln. In Kooperation von 28 Europäischen Nationen und der Europäischen Agentur für Netzwerksicherheit ENISA konnte dieses Wettbewerbsmodell als fixe Größe im europäischen Raum verankert werden.

Ziele der ECSC sind: Jugendliche für das Thema zu begeistern, sie bei ihrer Ausbildung zu fördern, sie bei ihren Karrierewegen unterstützen und Awareness für Cybersicherheit in Europa zu schaffen und zu erhöhen. Als Europäischer Leuchtturm-Bewerb soll die ECSC zudem die jeweiligen nationalen Organisationseinheiten in der Umsetzung ihrer nationalen Bewerbe unterstützen.

Beschreibung des Status

https://ecsc2022.eu / hhttps://ecsc2023.eu / https://ecsc.eu – das ECSC Finale wurde im September 2022 in Wien durchgeführt – Teams aus 33 Nationen ermittelten dabei den Europäischen Champion; Dänemark konnte sich vor Deutschland, Frankreich und Italien behaupten. Team Austria erreichte dabei wie schon beim Finale in Prag 2021 den 10. Rang. Die ECSC2023 wird von 23. bis 28.10 in Hamar/Norwegen durchgeführt. Österreich wird wieder mit einem Team vertreten sein.

Organisationsfeld

CSA – CyberSecurityAustria

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Bildung

Projekt: openECSC – Open European Cyber Security Challenge 2023

Start: 20.1.2023
Ende: 31.12.2023
Nr.: 4105

Aktuelles Jahr
Status: grün
Fortschritt: 35 %

Zugrundeliegende Strategische Ziele

Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

Die openEuropeanCyberSecurityChallenge dient dazu noch mehr Menschen für dieses Thema zu begeistern und die Zielsetzungen der ECSC nachhaltiger zu stärken. die Ergebnisse der openECSC2022 konnten ENISA überzeugen auch 2023 neben der ECSC wieder eine openECSC durchzuführen. Diese steht allen Securityinteressierten/spezialisten aus aller Welt offen und wird im Rahmen eines Online-Bewerbes in Trainingsrunden von März bis September 2023 durchgeführt und mit einem Online- Finale während des ECSC2023 Finales in Hamar gespielt.

Dies ist vor allem für die SecurityExperten vieler Unternehmen weltweit eine willkommene Gelegenheit ihr Können unter Beweis zu stellen – weshalb der Bewerb auch sehr großer Zusprache in diesem Teilnehmer-Segment erfährt

Beschreibung des Status

Die openECSC wird 2023 zum zweiten Mal ausgetragen und soll ab 2023 als fixer Bestandteil Europäischer Exzellenz-/Nachwuchsarbeit ebenso positioniert werden wie als Europäischer Leuchtturm der Sicherheitstalente aus allen Teilen der Welt nach Europa zu führt.

Das von CSA entwickelte Modell wird von ENISA und den Ländervertreter in den nächsten Jahren weiter ausbaut und in einen Regelbetrieb – analog ACSC/ECSC überführt werden. Zu den rund 20.000 Teilnehmenden Schülern und Studenten der ECSC sollen mittelfristig weitere 20.000 Spezialisten weltweit mit dem Format erreicht werden. CSA wurde seitens ENISA und Länder eingeladen hier in einem eigens geschaffene Exekutivkomittee weitere Entwicklungen voranzutreiben.

Organisationsfeld

CSA – CyberSecurityAustria

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Bildung

Projekt: FH OÖ – SSCCS (Secure Supply Chains for critical systems)

Start: 30.6.2021
Ende: 31.12.2024
Nr.: 4116

Aktuelles Jahr
Status: grün
Fortschritt: 80 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit
- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

- Projekt gestartet
- Supply Chain Use Cases abgeschlossen (Industrie, Logistik, Lebensmittelbereich, Pharma, Kritis)

Beschreibung des Status

- Projekt gestartet
- Supply Chain Use Cases abgeschlossen (Industrie, Logistik, Lebensmittelbereich, Pharma, Kritis)

Organisationsfeld

Fachhochschule Oberösterreich, Logistikum Steyr

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Kleine und mittlere Unternehmen (KMU)
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Bildung
- Forschung & Entwicklung

Projekt: FH OÖ – CySeReS-KMU

Start: 1.1.2023
Ende: 30.6.2025
Nr.: 4117

Aktuelles Jahr
Status: grün
Fortschritt: 70 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit
- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

Forschungsprojekt (Interreg Bayern – Österreich) zum Thema Supply Chain Cyber Security und Resilienz mit 4 Partneruniversitäten (Uni Passau, FH Deggendorf, Uni Innsbruck, FH Salzburg) mit Fokus auf KMU.

Beschreibung des Status

Projekt mit 1.1.2023 gestartet

Organisationsfeld

Fachhochschule Oberösterreich, Logistikum Steyr

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Kleine und mittlere Unternehmen (KMU)
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Bildung
- Forschung & Entwicklung

Projekt: FH OÖ – Sucredi

Start: 1.1.2019
Ende: 29.6.2022
Nr.: 4118

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit
- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

Forschungsprojekt zum Thema Supply Chain Cyber Resilienz begleitend zur Dissertation von Michael Herburger an der Copenhagen Business School. Das Projekt analysierte vier Supply Chains österreichischer Unternehmen. Output des Projektes ist u. a. ein Reifegradmodell zu „Supply Chain Cyber Resilience“. www.logistikum.at/sccr

Beschreibung des Status

Projekt abgeschlossen

- Reifegradmodell online verfügbar

Organisationsfeld

Fachhochschule Oberösterreich, Logistikum Steyr

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Kleine und mittlere Unternehmen (KMU)
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Bildung
- Forschung & Entwicklung

Projekt: AIT -Aufbau von Übungs- und Trainingsplattformen für Multistakeholder Infrastrukturszenarien

Start: 30.9.2022
Ende: 31.12.2024
Nr.: 4120

Aktuelles Jahr
Status: grün
Fortschritt: 70 %

Zugrundeliegende Strategische Ziele

- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen
- 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
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit

Gegenstand und Ziele

Realisierung von Simulationsmethoden und Werkzeugen für Szenarienanalysen von Abhängigkeiten verschiedener kritischen Infrastrukturen durch Cyber Security und Black-Out Szenarien

Beschreibung des Status

Erste spezielle Simulationsmethoden und -plattformen durch Technologie „made in Austria“ in Österreich am AIT etabliert und erste Multi-stakeholder Übungen der nationalen kritischen Infrastrukturbetreiber durchgeführt (z. B. KSÖ Black-Out Planspiel 2022).

Organisationsfeld

AIT

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Forschung & Entwicklung
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Bildung

Projekt: AIT – Realisierung von Cyber Security Schlüsseltechnologien made in Austria mit globalem Impact

Start: 1.1.2022
Ende: 31.12.2025
Nr.: 4121

Aktuelles Jahr
Status: grün
Fortschritt: 90 %

Zugrundeliegende Strategische Ziele

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

Gegenstand und Ziele

Entwicklung modernster Security by Design Entwicklungswerkzeuge „made in Austria“ für Märkte mit hohen Sicherheitsanforderungen.

Beschreibung des Status

Internationale Standardisierung für Cyber Security Zertifizierung im Automotive Bereich durch Österreich wesentlich beeinflusst und gestaltet. Globale führende Technologie „made in Austria“ am AIT umgesetzt. Globaler Systemvertrieb mit Industriepartner aus Österreich etabliert. Siehe AIT Technologie „Threatget“ – https://threatget.eu/

Organisationsfeld

AIT

Herausforderungen

Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Kleine und mittlere Unternehmen (KMU)

Projekt: AIT – Beitrag Österreichs zur Umsetzung des EU Cyber Resilience Acts

Start: 1.1.2022
Ende: 31.12.2026
Nr.: 4122

Aktuelles Jahr
Status: grün
Fortschritt: 70 %

Zugrundeliegende Strategische Ziele

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

- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen

Gegenstand und Ziele

Cyber Security by Design Produktentwicklungsmethoden für Industrie- und neue IoT Märkte zur Stärkung der digitalen Souveränität der EU

Beschreibung des Status

International führende Cyber Security by Design Produktentwicklungsmethoden und Werkzeuge für neue Digitalmärkte durch „made in Austria“ Technologieentwicklungen am AIT. Globale Vertriebskooperation mit AVL für den automotiv-Sektor umgesetzt. Tool für weitere Branchen erweitert.

Organisationsfeld

AIT

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Internationale Zusammenarbeit
- Forschung & Entwicklung
- Widerstandsfähigkeit

Projekt: AIT – Aufbau effektiver Threat-Intelligence Fähigkeiten für den Wirtschaftsstandort Österreich

Start: 1.1.2022
Ende: 31.12.2026
Nr.: 4123

Aktuelles Jahr
Status: grün
Fortschritt: 60 %

Zugrundeliegende Strategische Ziele

- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Gegenstand und Ziele

Entwicklung von Prozessen, Methoden und Werkzeugen zur Nutzung von Open Source Intelligence und Austausch im EU-Behördenverbund für den effektiven Betrieb von Security Operation Centers (SOC).

Beschreibung des Status

Internationale Vernetzung in der EU etabliert und erfolgreiche Kompetenz- und Technologieentwicklung für die NIS Behörde durch AIT erfolgt – Prototyp in Entwicklung (siehe EU CEF Telecom Call Projekt „Awake“)

Organisationsfeld

AIT

Herausforderungen

Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Forschung & Entwicklung
- Internationale Zusammenarbeit
- Widerstandsfähigkeit

Projekt: Mindsetters – Cyber-Awareness für Österreich – Produktname: „2b-aware“

Start: 31.7.2022
Ende: 1.5.2024
Nr.: 6123

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- In Österreich ist eine sichere Partizipation am gesellschaftlichen und politischen Leben im Cyberraum für Bürgerinnen und Bürger möglich

Gegenstand und Ziele

Das Ziel von „Cyber-Awareness für Österreich“ ist es, eine kostenlose, hochwertige Cybersecurity Awareness Schulung für jeden anzubieten, um dadurch das Bewusstsein für Gefahren im digitalen Raum zu schärfen. Basierend auf regelmäßig versendeten E-Mails werden Awareness-Inhalte auf verschiedene Weise und mit zusätzlichen Interaktionsmöglichkeiten kommuniziert.

Beschreibung des Status

Q3 2022: Plannungsbegin

- Dezember 2022: Definition der Anforderungen und technische Planung
- Mitte Jänner 2023: Entwicklungsbeginn
- Anfang Juli 2023: Alpha Status erreicht
- Ende August 2023: Start – Definition und Design der Inhalte und Implementierung in die Plattform
- 1.März: Beginn Testphase
- Anfang Mai: Abschluss und GoLive unter https://www.2b-aware.online/

Organisationsfeld

mindsetters GmbH

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Bewusstseinsbildung (Awareness)
- Kleine und mittlere Unternehmen (KMU)
- Bildung

Projekt: AKNOe -Onlinebetrug-Simulator

Start: 1.7.2021
Ende: 30.6.2022
Nr.: 6125

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

– Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
– Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
– Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;
– Österreich arbeitet in einem gesamtstaatlichen Ansatz stetig an der Weiterentwicklung seiner Rechtsgrundlagen zur Erhöhung der Cybersicherheit und Bekämpfung der Cyberkriminalität;

Gegenstand und Ziele

Der Onlinebetrug-Simulator ist ein Präventionsprojekt der AK Niederösterreich und der Universität Wien. Die Plattform https://onlinebetrug.aknoe.at dient als sichere Umgebung, um simulierten Online-Betrug „hautnah" zu erleben und Cyber-Kriminalität so aus einer ganz neuen Perspektive kennenzulernen. Und dabei nicht nur zu sehen, wie schnell man selber in die Falle tappt, sondern auch zu lernen, wie man genau das vermeidet.

Verschiedene interaktive Module ermöglichen das eigenständige Training samt individuellem Feedback, beispielsweise zu Fakeshops oder Phishing. Als Grundlage für das Projekt wurde eine Simulationsstudie zu Nutzer*innenverhalten in Fakeshops durchgeführt. Diese Studie ist hier abrufbar: https://noe.arbeiterkammer.at/beratung/konsumentenschutz/Fakeshop-Studie.pdf

Beschreibung des Status

• 01/2021 – 06/2021 Konzepterstellung
• 07/2021 Start des Projekts
• 07/2021 – 10/2021 Entwicklungsarbeiten für die Studienplattform (Simulationsstudie zu sicherheitsbewusstem Verhalten beim Online-Einkauf)
• 11/2021 – 12/2021 Durchführung der Nutzer*innen-Studie
• 11/2021 – 05/2022 Entwicklungsarbeiten für die Simulationsplattform
• 01/2022 – 02/2022 Studienauswertung
• 06/2022 Launch der Plattform onlinebetrug.aknoe.at

Organisationsfeld

AKNÖ/Universität Wien

Herausforderungen

– Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
– Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
– Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

– Vertrauen und Privatsphäre
– Bewusstseinsbildung (Awareness)
– Bildung
– Forschung & Entwicklung
– Widerstandsfähigkeit
– Cyberkriminalität und Strafverfolgung

Projekt: epicenter.academy: Digitale Selbstverteidigung

Start: 12.12.2022
Ende: 1.7.2028
Nr.: 6127

Aktuelles Jahr
Status: grün
Fortschritt: 50 %

Zugrundeliegende Strategische Ziele

- 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
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;

Gegenstand und Ziele

Mit der Ausbildungsreihe „Digitale Selbstverteidigung für Lehrlinge und Schüler:innen“ hat die epicenter.academy, unterstützt durch die AK NÖ, ein Trainingsprogramm für die junge Zielgruppe ausgearbeitet. Wir haben ein Train-the-Trainerprogramm entwickelt, Trainer:innen ausgebildet und angestellt, die aktiv altersgerecht weiterbilden können. Die Workshops konnten von den Schulen kostenlos abgerufen werden. Eine Webseite mit einem frei zugänglichen E-Learning (https://epicenter.academy/e-learning), das laufend aktualisiert und erweitert wird, ergänzt das Angebot. Die Inhalte sind in mittlerweile 12 Kapitel gegliedert. Es werden digitale Verschlüsselung, sichere Kommunikation, den Umgang mit Passwörtern,Phishing, die Gründe für Datenschutz und digitale Selbstverteidigung und mehr behandelt. Das Know-how wirkt Ängsten entgegen. Diese spezifische Qualifikation sorgt dafür, dass digitale Kommunikation und Tools sicher und selbstbestimmt genutzt werden.

Beschreibung des Status

Seit dem Start im Nov. 2022 haben wir in über 6000 Schüler:innen/Jugendliche zwischen 12 u. 19 Jahren in unterschiedlichen Standorten in NÖ, Wien u. der Steiermark erreicht. Mit dem Wintersemester 2024/25 haben wir unser Workshopangebot auf die Sekundarstufe 1 bzw. ab 12 Jahren erweitert. Durch die Förderung der AK OÖ wird in 2025 auch mit Workshops für das Bundesland OÖ gestartet. Unser offenes E-Learning wird außerdem vom BMBWF über die Eduthek.at auch für die Anwendung in der Oberstufe u. die Fortbildung von Lehrkräften empfohlen. Das frei zugängliche E-Learning wird, unterstützt durch eine Netidee Förderung, weiter ausgebaut. Auch der digitale Gewaltschutz in Form von Wissen u. Workshops für Frauenhäuser und Beratungsstellen wird 2025 ausgebaut.

Organisationsfeld

epicenter.academy GmbH – für digitale Kompetenz, Bildunsprojekt von epicenter.works- Plattform Grundrechtspolitik

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Bildung
- Kleine und mittlere Unternehmen (KMU)
- Vertrauen und Privatsphäre
- Bewusstseinsbildung (Awareness)
- Freier Meinungsbildungsprozess
- Ethik

Projekt: AIT – Österreich als aktiver EU Cyber Security Skill Development Stakeholder

Start: 1.6.2023
Ende: 31.12.2026
Nr.: 7131

Aktuelles Jahr
Status: grün
Fortschritt: 10 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- 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
- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen

Gegenstand und Ziele

Teilnahme Österreichs an der Etablierung und Umsetzung einer Infrastruktur in der EU zur Entwicklung von Cyber Security Skills und Competences für Unternehmen und Behörden; Positionierung des Standortes Wien im Eco-System zukünftiger EU Organisation in den EU MS.

Beschreibung des Status

Positionierung von Österreich als EU-weites Kompetenzzentrum für Capacity Building in der Industrie als auch SMEs und Behörden (berufliche Aus- und Weiterbildung). Positionierung von österreichischen Akteuren im Verbund von EU Stakeholdern im Kontext.

Organisationsfeld

BKA, AIT, AED

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Kleine und mittlere Unternehmen (KMU)
- Widerstandsfähigkeit
- Internationale Zusammenarbeit

Projekt: SV – Weiterentwicklung SV-Sicherheitsstandards

Start: 1.10.2022
Ende: 31.3.2024
Nr.: 7132

Aktuelles Jahr
Status: grün
Fortschritt: 80 %

Zugrundeliegende Strategische Ziele

- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- 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
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- In Österreich ist eine sichere Partizipation am gesellschaftlichen und politischen Leben im Cyberraum für Bürgerinnen und Bürger möglich

Gegenstand und Ziele

Zweck der Sicherheitsrichtlinie für die gesetzliche Sozialversicherung (SV-SR) ist es, eine für alle SV-Organisationen einheitliche Vorgangsweise bei folgenden Sicherheitsthemen zu erreichen:

1. Risikomanagement der Informationssicherheit
2. Informationssicherheit
   - CISO je SV-Organisation vorgeschrieben
   - SV-CISO Community (C2; Sicherheitsgremium)
   - SV-CERT (zentrale Melde- und Koordinierungsstelle bei Vorfällen)
   - jährliches Sicherheitsgesamtbild aller SV-Organisationen
3. Krisenmanagement

in 2023 werden folgende SV-Standards überarbeitet bzw. neu erstellt:

- SV-Handbuch sichere Software Entwicklung
- SV-Handbuch BCM
- SV-Handbuch Risikomanagement (inkl. einheitlicher Gefahrenliste)

Beschreibung des Status

Beginn Erstellung und/oder Überarbeitung mit Experten in Arbeitsgruppen

- Präsentation in der C2
- Qualitätssicherung
- Freigabe durch C2
- Freigabe durch Direktoren und Konferenz-Beschluss
- Veröffentlichung im SV-Intranet

Organisationsfeld

Dachverband der SV-Träger

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Internationale Zusammenarbeit
- Widerstandsfähigkeit
- Vertrauen und Privatsphäre

Projekt: FH JOANNEUM – Masterstudium IT & Mobile Security

Start: 1.1.2001
Ende: 31.12.2099
Nr.: 7133

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Master: IT & Mobile Security – Berufsbegleitende

Master: IT-Recht & Management – Berufsbegleitend

Zugrundeliegende Strategische Ziele

- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit

Gegenstand und Ziele

Fachhochschulausbildung im Bereich Cyber Security: Das Institut Software Design und Security der FH JOANNEUM ist am Standort Kapfenberg angesiedelt. Die Studiengänge des Instituts beschäftigen sich mit vielen verschiedenen Bereichen der Informatik und natürlich mit den damit verbundenen Anwendungsmöglichkeiten.

Die IT-Security Grundausbildung ist in den Bachelor Studiengängen bereits fest verankert:

Bachelor: Software Design & Cloud Computing – Vollzeit

Bachelor: Software Design & Cloud Computing – Berufsbegleitend

Bachelor: Mobile Software Development – Dual

Zusätzlich bieten zwei Masterstudiengänge weiterführende Kompetenzen und Spezialisierungen an:

Beschreibung des Status

2001: Start des Diplomstudiums „Internettechnik & Management“ – Vollzeit

2004: Erweiterung des Studiums um die berufsbegleitende Vertiefung „Software Design“

2006: Start des berufsbegleitenden Masterstudiums „Advanced Security Engineering“

2008: Start des berufsbegleitenden Masterstudiums „IT Recht & Management“

2014: Anpassung des Masterstudiums „Advanced Security Engineering“ → „IT & Mobile Security“

2018: Start des dual Bachelor Studiums „Mobile Software Development“

2020: Anpassung „Internet Technik & Management“ → „Software Design & Cloud Computing“ Vollzeit und Berufsbegleitend

2024: Anpassung des Masterstudiums „IT & Mobile Security“ – neues Curriculum

2024: Anpassung des Masterstudiums „IT Recht & Management“ – neues Curriculum

Organisationsfeld

FH JOANNEUM Institut Software Design & Security

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

- Bildung
- Wirtschaftsstandort
- Bewusstseinsbildung (Awareness)

Projekt: FH JOANNEUM – CyMoDACS: Cyber-Security and Mobility for Digital Aeronautic Communication Systems

Start: 1.1.2022
Ende: 30.6.2025
Nr.: 7134

Aktuelles Jahr
Status: grün
Fortschritt: 80 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit

Gegenstand und Ziele

FFG Takeoff: Im Single European Sky ATM Research Programme (SESAR) wird aktuell eine Air-Traffic-Management (ATM) Modernisierung durchgeführt, die deren Digitalisierung und verstärkte Automatisierung zum Ziel hat, um eine leistungsfähige und effiziente Luftfahrt zu gewährleisten. Der dazu notwendige digitale Flugfunk soll mit der vielversprechenden neuen Technologie LDACS (L-band Digital Aeronautical Communications System) realisiert werden. Die in dem Vorhaben CyMoDACs erzielten Ergebnisse sollen die Einführung von LDACS entscheidend voranbringen. Ein wesentlicher Aspekt, der in diesem Vorhaben adressiert wird, ist die Erweiterung des aktuellen LDACS Standards durch cyber-sichere Protokolle und die Erarbeitung einer Feinspezifikation für IPv6-Mobilität, die für einen Datenlink als Voraussetzung gilt, um diesen in der Luftfahrt einsetzten zu können.

Beschreibung des Status

Im Rahmen des Projekts wird LDACS entsprechend optimiert, damit die für die Mobilität benötigten Protokolle cyber-sicher sind und die System Performance beim Zellenwechsel (Handover) gewährleistet ist. Die geplante LDACS-Referenzimplementierung und Validierung der Interoperabilität erhöhen den Reifegrad des Gesamtsystems und fördern die Standardisierung in der Internationalen Zivilluftfahrtorganisation (ICAO). Die aufzubauende LDACS-Bodeninfrastruktur für den prä-operationellen Testbetrieb unterstützt die LDACS-Validierung, die in SESAR durchgeführt werden muss und erlaubt eine erste Überprüfung der LDACS Betriebs- und Transition-Konzepte, die für die Akzeptanz in der Luftfahrt und damit für die Markteinführung entscheidend sind.

Organisationsfeld

FH JOANNEUM Institut Software Design & Security

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Forschung & Entwicklung

Projekt: FH JOANNEUM – CSecTOR

Start: 1.12.2022
Ende: 30.11.2024
Nr.: 7135

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen
- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

Gegenstand und Ziele

EU Erasmus+: CSecTOR ist ein europäisches Erasmus-Projekt, das Unternehmen, insbesondere KMUs, dabei hilft, das Risiko von Cyberangriffen zu minimieren. Durch eine interaktive Online-Schulungsplattform werden Schulungsmaterialien und Methoden bereitgestellt, um das Bewusstsein für Cybersicherheit zu erhöhen und Abwehrstrategien zu entwickeln.

Beschreibung des Status

abgeschlossen

Organisationsfeld

FH JOANNEUM Institut Software Design & Security

Herausforderungen

- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Kleine und mittlere Unternehmen (KMU)

Regulatoren

Projektverantwortliches Ressort
Staatliche Regulierungsbehörden

Stand: 5.3.2025

Nr.	Projekt	Status	Fortschritt / Projektampel	Start	Ende
1	E-Control Energie-Branchenrisikoanalyse	grün	90 %	1.1.2024	31.3.2025
2	FMA – Assessment der Mitigationsmaßnahmen	grün	60 %	1.1.2024	31.12.2099
3	FMA – DORA-Gap-Analyse	grün	60 %	1.1.2024	31.12.2099
4	FMA – DORA-Beaufsichtigung	grün	100 %	8.2.2024	31.12.2099
5	FMA – IT Governance Einsichtnahmen	grün	100 %	30.9.2023	31.12.2099
6	E-Control – Umsetzung Network Code Cyber Security	grün	5 %	12.6.2024	31.12.2028
7	E-Control: Gemeinsame Übung Cyber Europe	grün	100 %	18.6.2024	20.6.2024
8	FMA – Cyber Maturity Level Assessment	grün	70 %	1.1.2022	31.12.2099
9	FMA, OeNB – Vor-Ort-Prüfungen bei den beaufsichtigten Finanzunternehmen	grün	100 %	30.6.2018	31.12.2099
10	FMA – Blackout Maturity Level Assessment	grün	80 %	20.1.2022	31.12.2099
11	FMA – Cyber Security Exercise	grün	60 %	1.1.2022	31.12.2099
12	RTR – Hochrisikolieferanten	grün	100 %	1.1.2022	31.12.2099
13	RTR – 5G Sicherheit	grün	100 %	1.1.2022	15.6.2022
14	RTR – Informationssicherheitsmanagement und Sicherheitsstandards	grün	100 %	1.1.2022	15.6.2022
15	RTR – TK-Branchenrisikoanalyse (TK-BRA)	grün	100 %	1.1.2022	15.6.2022
16	RTR – TK Cybersecurity Expertengruppe	grün	100 %	1.1.2022	1.1.2099
17	RTR – Behördentreffen IT-Risiko	grün	100 %	1.1.2022	31.12.2099
18	RTR – Mustersicherheitskonzept	grün	10 %	1.1.2022	15.6.2026
19	RTR – Vernetzung mit E-Wirtschaft	grün	100 %	1.1.2022	31.12.2099

Projekt: E-Control Energie-Branchenrisikoanalyse

Start: 1.1.2024
Ende: 31.3.2025
Nr.: 7152

Aktuelles Jahr
Status: grün
Fortschritt: 90 %

Beschreibung des Status

für 2022 abgeschlossen; nächste Aktualisierung 2024/25 Beginn 2024, Fertigstellung 2025

Zugrundeliegende Strategische Ziele

- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Organisationsfeld

e-Control

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Gegenstand und Ziele

Entsprechend der Empfehlungen aus ÖSCS und APCIP hat die E-Control zum wiederholten Male gemeinsam mit dem Sektor eine Branchenrisikoanalyse durchgeführt. Hierbei nehmen Experten aus Bundesministerien, Sektorenvertreter und Interessenvertretungen eine Analyse der Risiken im Sektor vor und leitet Maßnahmenempfehlungen für die Stakeholder ab. Eine Aktualisierung findet im Abstand von 2–3 Jahren statt, die nächste Aktualisierung der Branchenrisikoanalyse ist für 2024/2025 geplant (Beginn 2023, Fertigstellung 2024).

Zielgruppe & Themenbereiche

- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Wirtschaftsstandort
- Kleine und mittlere Unternehmen (KMU)
- Widerstandsfähigkeit

Projekt: FMA – Assessment der Mitigationsmaßnahmen

Start: 1.1.2024
Ende: 31.12.2099
Nr.: 8149

Aktuelles Jahr
Status: grün
Fortschritt: 60 %

Zugrundeliegende Strategische Ziele

- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

Ziel ist die Evaluierung der Sicherheitsmaßnahmen (Mitigations & Detections), die die beaufsichtigten Unternehmen zur Bewältigung eines aktuellen (von der FMA ausgewählten) Cyberangriffsszenarios gesetzt haben. Die Struktur des Assessments folgt den Taktiken (Ziele der Angreifer) und Techniken (Mittel der Eingreifer zur Zielerreichung) von MITRE ATT&CK. Unternehmen können somit das Assessment nutzen, um die eigenen Sicherheitsmaßnahmen mit jenen der anderen Unternehmen zu vergleichen und die Quellen auch für eigene weiterführende Analysen heranzuziehen.

Beschreibung des Status

- Entwicklung und erstmalige Durchführung im Versicherungssektor (2023)
- Bilaterale Feedback-Gespräche mit den Unternehmen auf Management-Ebene (2024)
- Berücksichtigung der Erkenntnisse im Risikoscoring (2024)

Organisationsfeld

FMA

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

Betreiber wesentlicher Dienste und kritischer Infrastrukturen

Projekt: FMA – DORA-Gap-Analyse

Start: 1.1.2024
Ende: 31.12.2099
Nr.: 8150

Aktuelles Jahr
Status: grün
Fortschritt: 60 %

Zugrundeliegende Strategische Ziele

- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

Der Umsetzungsstand zur Erfüllung der künftigen DORA-Erfordernisse wird anhand eines strukturierten Assessment-Tools eruiert (DORA, digital operational resilience for the financial sector).

Beschreibung des Status

- Entwicklung und erstmalige Durchführung (2024)
- Bilaterale Feedback-Gespräche mit den Unternehmen auf Management-Ebene (2024)
- Berücksichtigung der Erkenntnisse im Risikoscoring (2025)

Organisationsfeld

FMA

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

Betreiber wesentlicher Dienste und kritischer Infrastrukturen

Projekt: FMA – DORA-Beaufsichtigung

Start: 8.2.2024
Ende: 31.12.2099
Nr.: 8151

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

Seit 17.1.2025 gelten die Vorgaben über die digitale operationale Resilienz im Finanzsektor (DORA, digital operational resilience for the financial sector). Ziel der FMA ist, DORA zu vollziehen bzw. die Umsetzung der DORA-Vorgaben durch Finanzunternehmen zu beaufsichtigen. Damit verbundene Ziele:

1. Strategische Planung und Steuerung der FMA-DORA-Ziele, -Aufsichtsschwerpunkte und -Tätigkeiten
2. Abstimmung von FMA-Positionen zu DORA auf europäischer und nationaler Ebene sowie Sicherstellung einheitlicher Rechtsauslegungen und aufsichtlicher Erwartungshaltungen für den DORA-Vollzug
3. DORA-Vollzug iSd integrierten Aufsichtsansatzes
4. Externe Kommunikationsmaßnahmen sowie FMA-interner Wissenstransfer

Beschreibung des Status

- Einbezug von DORA-Aufsichtsaufgaben in die strategische Planung und Steuerung
- FMA-Vertretung von abgestimmten Positionen zu DORA in nationalen und europäischen Gremien
- DORA-Vollzug, inkl. diesbezüglicher Koordinierungen
- Laufende externe Kommunikationsmaßnahmen sowie FMA-interner Wissenstransfer

Organisationsfeld

FMA

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

Betreiber wesentlicher Dienste und kritischer Infrastrukturen

Projekt: FMA – IT Governance Einsichtnahmen

Start: 30.9.2023
Ende: 31.12.2099
Nr.: 8152

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

Im Rahmen von IT Governance Einsichtnahmen wird im Rahmen von physischen Terminen die IT-Governance von ausgewählten Instituten (LSI) evaluiert. Ziel ist der Dialog mit beaufsichtigten Unternehmen und das Aufzeigen von möglichen Optimierungsmaßnahmen der IT-Governance von Unternehmen und damit einer Verbesserung der Resilienz gegen IT-Risiken.

Beschreibung des Status

laufende Tätigkeit

Organisationsfeld

FMA

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

Betreiber wesentlicher Dienste und kritischer Infrastrukturen

Projekt: E-Control – Umsetzung Network Code Cyber Security

Start: 12.6.2024
Ende: 31.12.2028
Nr.: 9191

Aktuelles Jahr
Status: grün
Fortschritt: 5 %

Beschreibung des Status

Der NCCS ist seit 13.Juni 2024 in Kraft und die Umsetzung hat begonnen.

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ausreichend finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, zu erkennen und sie abzuwehren
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;
- 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

Organisationsfeld

E-Control

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Betreiber wesentlicher Dienste und kritischer Infrastrukturen

Gegenstand und Ziele

Der Network Code Cyber Security (NCCS) gilt für critical und high impact entities im Stromsektor und soll die Cyberresilienz vor allem grenzüberschreitend sicherstellen. Die E-Control definiert Maßnahmen und stellt gemeinsam mit den regulierten Unternehmen sicher, dass der NCCS angemessen umgesetzt wird.

Projekt: E-Control: Gemeinsame Übung Cyber Europe

Start: 18.6.2024
Ende: 20.6.2024
Nr.: 9192

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Gegenstand und Ziele

Die E-Control hat gemeinsam mit der Energiewirtschaft an der europaweiten Cyber-Übung Cyber Europe der ENISA teilgenommen.

Beschreibung des Status

Die Teilnahme an der Übung wurde abgeschlossen.

Organisationsfeld

E-Control, Behörden, Energiewirtschaft

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Widerstandsfähigkeit
- Cyberverteidigung
- Internationale Zusammenarbeit

Projekt: FMA – Cyber Maturity Level Assessment

Start: 1.1.2022
Ende: 31.12.2099
Nr.: 4106

Aktuelles Jahr
Status: grün
Fortschritt: 70 %

Zugrundeliegende Strategische Ziele

- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

Zur Evaluierung der Verwundbarkeit der beaufsichtigten Unternehmen gegenüber dem IKT-Risiko hat die FMA als 1. Behörde in der EU ein Tool zur Ermittlung der Cyber Resilienz der Unternehmen am Finanzmarkt entwickelt und setzt dieses seit 2019 im Versicherungs- und Pensionskassensektor ein.

Dieses Assessment ermöglicht der FMA, die Cyberresilienz zu messen und die Reifegrade der einzelnen beaufsichtigten Unternehmen zu ermitteln und in das Risikoscoring zu integrieren. Das Tool dient den Unternehmen auch als Hilfestellung, um ihre Cyber Resilienz zu verbessern.

Beschreibung des Status

- Entwicklung und erstmalige Durchführung des Cyber Maturity Level Assessments im Versicherungssektor (2019)
- Durchführung im Pensionskassensektor (2020)
- Ausrollung auf anderen Sektoren des Finanzmarktes (2021)
- Bilaterale Feedback-Gespräche mit den Unternehmen auf Management-Ebene (2022)
- Berücksichtigung der Erkenntnisse bei der Cyber Exercise und dem Assessment der Mitigationsmaßnahmen (2023)
- Künftige Ausrollung auf andere Sektoren (BVK)

Organisationsfeld

FMA

Herausforderungen

- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

Betreiber wesentlicher Dienste und kritischer Infrastrukturen

Projekt: FMA, OeNB – Vor-Ort-Prüfungen bei den beaufsichtigten Finanzunternehmen

Start: 30.6.2018
Ende: 31.12.2099
Nr.: 4107

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

Die Finanzmarktaufsichtsbehörde führt bei den von ihr beaufsichtigten Finanzunternehmen Vor-Ort-Prüfungen zum Thema IT-Sicherheit mit dem Fokus Cyber-Security durch. Es handelt sich dabei um einen FMA-weiten Aufsichtsschwerpunkt. Im Bereich der Bankenaufsicht (betrifft Significant Institutions (SI) und Less Significant Institutions (LSI)) werden die Vor-Ort-Prüfungen von der Oesterreichischen Nationalbank durchgeführt. Die Prüfungen folgen aufsichtlichen Vorgaben sowie internationalen Prüf- und Kontrollstandards. Ziel der Vor-Ort-Prüfungen ist es, die IT-Sicherheit und Resilienz der Unternehmen zu stärken.

Beschreibung des Status

- Entwicklung Prüfmethodik im Bankensektor 2010, erste Prüfungen 2012
- Entwicklung Prüfmethodik im Versicherungs- und Pensionskassensektor und erste Prüfungen 2018
- Entwicklung Prüfmethodik im Wertpapiersektor und erste Prüfungen 2019
- Ableitung von Handlungsempfehlungen und Rückmeldungen an die beaufsichtigten Unternehmen in bilateralen Feedbackgesprächen
- Basis für weitere aufsichtliche Maßnahmen
- gesteigerte Intensität von Prüfungen des IT-Risikos bei SI
- Weiterentwicklung und Integration neuer regulatorischen Vorgaben am Finanzmarkt (insb. DORA)
- Weiterer Ausbau der IT-Prüfungen im LSI-Bereich

Organisationsfeld

FMA, OeNB

Herausforderungen

Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

Betreiber wesentlicher Dienste und kritischer Infrastrukturen

Projekt: FMA – Blackout Maturity Level Assessment

Start: 20.1.2022
Ende: 31.12.2099
Nr.: 4108

Aktuelles Jahr
Status: grün
Fortschritt: 80 %

Zugrundeliegende Strategische Ziele

- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

Zur Evaluierung der Verwundbarkeit der beaufsichtigten Unternehmen gegenüber dem Risiko und den Folgen eines Blackouts, also eines länger andauernden, weite Teile Europas betreffenden Strom-, Infrastruktur- und Versorgungsausfalls, hat die FMA Anfang 2022 ein Blackout Maturity Level Assessment entwickelt und zunächst im Pensionskassensektor sowie Versicherungssektor durchgeführt.

Mit diesem Aufsichtstool verfolgt die FMA folgende Ziele:

- die Marktteilnehmer für die Risiken eines Blackout zu sensibilisieren,
- Bewusstsein zu schaffen und die rechtzeitige Vorbereitung auf das Szenario eines Blackouts aktiv voranzutreiben.

Das Blackout-Risiko-Assessment der FMA beurteilt den Reifegrad der Maßnahmen in drei Phasen: der Vorbereitung auf einen möglichen Blackout, die Bewältigung und Reaktion bei einem Blackout sowie das Wiederanlaufen und die Wiederherstellung des Betriebes nach einem Blackout.

Beschreibung des Status

Das Blackout-Risiko-Assessment der FMA beurteilt den Reifegrad der durch Finanzmarktteilnehmer getroffenen Maßnahmen in drei Phasen: der Vorbereitung auf einen möglichen Blackout, die Bewältigung und Reaktion bei einem Blackout sowie das Wiederanlaufen und die Wiederherstellung des Betriebes nach einem Blackout.

- Entwicklung und erste Durchführung im Pensionskassensektor 2022
- Ausrollen auf den Versicherungssektor (2023) sowie künftig ggf. auf andere Sektoren des Finanzmarktes (BVK)

Organisationsfeld

FMA

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

Betreiber wesentlicher Dienste und kritischer Infrastrukturen

Projekt: FMA – Cyber Security Exercise

Start: 1.1.2022
Ende: 31.12.2099
Nr.: 4119

Aktuelles Jahr
Status: grün
Fortschritt: 60 %

Zugrundeliegende Strategische Ziele

- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;

Gegenstand und Ziele

In der „Cyber Exercise“ evaluiert die FMA auf Basis einer realitätsnahen Simulation eines Cyberangriffs die Angemessenheit der auf die Injects (auf die teilnehmenden Unternehmen zugeschnittene Informationsfragmente, z. B. E-Mails, Telefonanrufe, Nachrichten) in Echtzeit folgenden Reaktionen der teilnehmenden Versicherungsunternehmen.

Die Aufgabe der teilnehmenden Unternehmen bei diesem „Real time-Test“ ist, diese Injects unter Zeitdruck zu analysieren und in einem sehr knapp bemessenen Zeitrahmen auf jeden Inject angemessene Reaktionen zum Schutz und zur Absicherung der Informations- und Kommunikationstechnologie (IKT) zu definieren. Am Ende der Übung sind IKT-Vorfallsmeldungen zu erstellen, die dann analysiert und geprüft werden.

Beschreibung des Status

- Entwicklung und erstmalige Durchführung im Versicherungssektor (2023)
- Bilaterale Feedback-Gespräche mit den Unternehmen auf Management-Ebene (2024)
- Berücksichtigung der Erkenntnisse im Risikoscoring (2024)
- Ausrollung auf andere Sektoren geplant (BVK)

Organisationsfeld

FMA

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

Betreiber wesentlicher Dienste und kritischer Infrastrukturen

Projekt: RTR – Hochrisikolieferanten

Start: 1.1.2022
Ende: 31.12.2099
Nr.: 2098

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- 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

Gegenstand und Ziele

Der Beirat für Sicherheit in elektronischen Kommunikationsnetzen gem. § 45 TKG 2021 dient dem zuständigen Bundesministerium als Beratungsgremium in Fragen der Cybersicherheit und als Expertengremium zur Erstellung von Gutachten im Zuge der Einstufung eines Herstellers als „Hochrisikolieferant“. Die RTR führt den Vorsitz und dient als Geschäftsstelle des Beirats.

Beschreibung des Status

- Laufende Tätigkeit
- Jährlich: Wahrnehmungsbericht
- Im Falle der Beauftragung durch den Bundesminister für Finanzen: Gutachten zur Einstufung eines Unternehmens als Hochrisikolieferant

Organisationsfeld

RTR

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Kleine und mittlere Unternehmen (KMU)
- Widerstandsfähigkeit
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen

Projekt: RTR – 5G Sicherheit

Start: 1.1.2022
Ende: 15.6.2022
Nr.: 2100

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Gegenstand und Ziele

Der Maßnahmenkatalog der EU 5G Cybersecurity Toolbox trägt der Bedeutung von 5G Netzen und Diensten Rechnung und wurde durch die TK-Netzsicherheitsverordnung 2020 (TK-NSiV 2020) der RTR in nationales Recht umgesetzt. Der RTR obliegt damit die Aufsicht in Fragen der Sicherheit von 5G.

Beschreibung des Status

- TK-Netzsicherheitsverordnung 2020 in Kraft
- Einmeldungen von Betreibern gem. TK-NSiV 2020 erfolgen nach Plan

Organisationsfeld

RTR

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Kleine und mittlere Unternehmen (KMU)
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Widerstandsfähigkeit

Projekt: RTR – Informationssicherheitsmanagement und Sicherheitsstandards

Start: 1.1.2022
Ende: 15.6.2022
Nr.: 2101

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Gegenstand und Ziele

Die TK-Netzsicherheitsverordnung sieht das Monitoring der von Anbietern und Betreibern obligatorisch vorzusehenden Maßnahmen des Informationssicherheits-Management und der Einhaltung der relevanten Sicherheitsstandards durch die RTR vor.

Beschreibung des Status

- TK-Netzsicherheitsverordnung 2020 in Kraft
- Einmeldungen von Betreibern gem. TK-NSiV 2020 erfolgen nach Plan

Organisationsfeld

RTR

Herausforderungen

- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Kleine und mittlere Unternehmen (KMU)
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Widerstandsfähigkeit

Projekt: RTR – TK-Branchenrisikoanalyse (TK-BRA)

Start: 1.1.2022
Ende: 15.6.2022
Nr.: 2102

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- 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

Gegenstand und Ziele

Entsprechend der Empfehlungen aus ÖSCS und APCIP hat die RTR zum wiederholten Male gemeinsam mit dem Sektor eine Branchenrisikoanalyse durchgeführt. Hierbei nehmen Experten aus Bundesministerien, TK-Netzbetreibern und -Diensteanbietern, Interessenvertretungen und der Internet-Community eine Analyse der Risiken im Sektor vor und leiten Maßnahmenempfehlungen für die Stakeholder ab. Eine Aktualisierung findet im Abstand von 2 Jahren statt. Die nächste Aktualisierung der Branchenrisikoanalyse ist für 2026 geplant.

Beschreibung des Status

Nächste Aktualisierung für 2026 geplant

Organisationsfeld

RTR

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Kleine und mittlere Unternehmen (KMU)
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Widerstandsfähigkeit

Projekt: RTR – TK Cybersecurity Expertengruppe

Start: 1.1.2022
Ende: 1.1.2099
Nr.: 2103

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- 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

Gegenstand und Ziele

Im Zuge der Arbeiten an der TK-Branchenrisikoanalyse konnte die RTR eine Expertengruppe für das Thema Netzsicherheit etablieren, die auch abseits der Branchenrisikoanalysen angerufen werden kann und sich mit aktuellen Themen der Sicherheit befasst.

Beschreibung des Status

Laufende Tätigkeit

Organisationsfeld

RTR

Herausforderungen

- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Kleine und mittlere Unternehmen (KMU)
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Widerstandsfähigkeit

Projekt: RTR – Behördentreffen IT-Risiko

Start: 1.1.2022
Ende: 31.12.2099
Nr.: 2104

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;

Gegenstand und Ziele

Das Behördentreffen IT-Risiko ist eine Vernetzung auf Behördenebene, welcher derzeit FMA, BWB, E-Control, Schienen-Control, APAB und RTR angehören und einen regelmäßigen Austausch zu Sicherheitsthemen gewährleisten.

Beschreibung des Status

Laufende Tätigkeit

Organisationsfeld

RTR

Herausforderungen

- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Kleine und mittlere Unternehmen (KMU)
- Wirtschaftsstandort

Projekt: RTR – Mustersicherheitskonzept

Start: 1.1.2022
Ende: 15.6.2026
Nr.: 2105

Aktuelles Jahr
Status: grün
Fortschritt: 10 %

Zugrundeliegende Strategische Ziele

- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen

Gegenstand und Ziele

Die RTR hat in Zusammenarbeit mit der ISPA eine Mustervorlage für ein Sicherheitskonzept erarbeitet, welches speziell kleineren und mittleren Betreibern dabei behilflich sein soll, gesetzlichen Vorgaben hinsichtlich der Integrität und Sicherheit von Netzen nach § 44 Abs 3 TKG 2021 bzw. § 5 Abs. 2 Telekom-Netzsicherheitsverordnung umzusetzen.

Beschreibung des Status

- Überarbeitung des Mustersicherheitskonzepts im Hinblick auf NIS2 gemeinsam mit ISPA nach Inkrafttreten des NISG 2025

https://www.ispa.at/wissenspool/vorlagen/ispa-mustersicherheitskonzept/

Organisationsfeld

RTR

Herausforderungen

- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Kleine und mittlere Unternehmen (KMU)
- Wirtschaftsstandort

Projekt: RTR – Vernetzung mit E-Wirtschaft

Start: 1.1.2022
Ende: 31.12.2099
Nr.: 2106

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;
- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- 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

Gegenstand und Ziele

Zur Adressierung gemeinsamer Risiken sowie Kaskadeneffekten von TK- und Energiebranche haben RTR und Vertreter der E-Wirtschaft eine Vernetzung hergestellt, die sich regelmäßig mit gemeinsamen Sicherheitsfragen auseinandersetzt.

Beschreibung des Status

Laufende Tätigkeit

Organisationsfeld

RTR

Herausforderungen

- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Wirtschaftsstandort
- Kleine und mittlere Unternehmen (KMU)
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Widerstandsfähigkeit

Sub-Projekt: RTR – Anlassbezogene Workshops zu aktuellen Bedrohungen (z. B. SS7, FluBot/Malware, usw.)

Start: 1.1.2022
Ende: 31.12.2099
Nr.: 2107

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Zugrundeliegende Strategische Ziele

- Österreich arbeitet stark und aktiv auf nationaler, europäischer und internationaler Ebene im Cyberbereich zusammen
- 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
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert;

Gegenstand und Ziele

Die RTR lädt Sicherheitsexperten der TK-Branche anlassbezogen zu Besprechungen und Workshops um gemeinsam anstehende Herausforderungen zu analysieren und mögliche Maßnahmen zu erörtern.

Beschreibung des Status

Laufende Tätigkeit

Organisationsfeld

RTR

Herausforderungen

- Bedrohungen, die mit der sachgemäßen Nutzung und der Abhängigkeit von IT einhergehen
- Bedrohungen, die mit der missbräuchlichen Nutzung von Informationstechnologie (IT) einhergehen
- Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

- Widerstandsfähigkeit
- Betreiber wesentlicher Dienste und kritischer Infrastrukturen
- Kleine und mittlere Unternehmen (KMU)
- Wirtschaftsstandort