Maßnahmenkatalog der Österreichischen Strategie für Cybersicherheit 2021

Fortschrittsbericht 1/2024

Maßnahmenkatalog der Österreichischen Strategie für Cybersicherheit 2021

Fortschrittsbericht 1/2024

Wien, 2024

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundeskanzleramt, Ballhausplatz 2, 1010 Wien
Telefon: +43 1 531 15-123456
bundeskanzleramt.gv.at
Wien, 2024

Inhalt

Präambel 4

Aufbau der ÖSCS 2021 4

Fortschrittsmessung 5

Bericht der Cyber Sicherheit Plattform 7

Projektübersicht 8

Auswertung für: Alle Ressorts 13

BKA 15

BMF 33

BMBWF 40

BMI 43

BMJ 56

BMLV 59

BMEIA 78

BMAW 85

BMK 96

BMKOES 98

BMSGPK 100

CSP/PPP 106

Regulatoren 168

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, webseitengestützen 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 11. März 2024 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: 11.3.2024

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: 11.3.2024

Ressort	Project	Start	Ende	Fortschritt
BKA	Aufbau NCC	27.6.2021	31.8.2025	90 %
BMF	ID Austria / E-ID	30.11.2021	29.7.2022	100 %
BMLV	Ausbau und verstärkte EU-Koordinierung nationaler milCERTs (Beitrag zum CDPF-Review der EU)	9.9.2021	31.12.2024	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	31.12.2023	100 %
BMEIA	Teilnahme an Forschungs- und Entwicklungsprojekten	31.8.2021	30.4.2025	85 %
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	30%
BMAW	[PRÄS] Konzept für Cybersicherheits-Berichtswesen (IKT-W)	1.1.2022	31.3.2024	90 %
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	31.12.2023	80%
BMSGPK	IT-System zur Erkennung von sicherheitskritischen Ereignissen (SIEM) gemäß Etappenplan	1.2.2023	15.12.2024	80%
BMSGPK	Etablierung Leitlinien Risikomgmt. in der Netz- und Informationssicherheit	1.2.2023	30.9.2024	80%

Ressort	Project	Start	Ende	Fortschritt
BMSGPK	Weiterentwicklung des Informationssicherheitsmanagement (ISMS) Tools	1.2.2023	31.12.2024	70%
BMAW	[PRÄS] Aktualisierung der IS-Richtlinie (IKT-W)	30.4.2023	31.3.2024	90%
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%
BMLV	Umsetzung der EU Cyber Defence Policy	10.7.2023	31.12.2025	10%
Regulatoren	E-Control Energie-Branchenrisikoanalyse	1.1.2024	31.3.2025	10%
BKA	Vorantreiben Einrichtung Cyber Rapid Response Teams	21.2.2024	1.1.2099	20%
Regulatoren	FMA – Assessment der Mitigationsmaßnahmen	1.1.2024	31.12.2099	100%
Regulatoren	FMA – DORA-Gap-Analyse	1.1.2024	31.12.2099	20%
Regulatoren	FMA – DORA-Implementierung	8.2.2024	31.12.2025	20%
Regulatoren	FMA – IT Governance Deep Dives	30.9.2023	31.12.2099	50%
BMSGPK	Erstellung eines Maßnahmenplans zur Netz- und Informationssicherheit	1.1.2024	30.9.2024	30%
BMF	oesterreich.gv.at / App Digitales Amt	30.11.2021	29.4.2022	100%
BMI	Ausbau C 4 zu moderner High Tech Einheit	1.1.2021	30.6.2024	65%
BMLV	Durchführung von Forschungs- und Entwicklungsprojekten im nationalen und EU-Kontext	23.11.2021	31.12.2032	55%
Regulatoren	FMA – Cyber Maturity Level Assessment	1.1.2022	31.12.2099	100%
BKA	Umsetzung NIS 2 Richtlinie	16.1.2023	15.10.2024	60%
CSP/PPP	Uni Wien – DaTra	1.12.2022	31.1.2024	100%
BKA	Etablierung CISO in den Bundesministerien	15.12.2020	31.12.2023	100%
BMF	Ausweisplattform	30.11.2021	31.12.2022	100%
BMI	Umsetzung und/oder funktionelle Erweiterungen der IKT-Lösungen gem. NISG	1.1.2021	30.9.2027	45%
BMLV	Informationsgenerierung und Einbringen militärpolitischer Positionen in VN, NATO, OSZE und EU	19.3.2013	31.12.2029	85%
BKA	Ausbau des ZAS Lagezentrums zu einem IKDOK Ausweichlagezentrum	31.5.2022	31.12.2023	100%
Regulatoren	FMA – Vor-Ort-Prüfungen bei den beaufsichtigten Finanzunternehmen	30.6.2018	31.12.2099	100%
CSP/PPP	SBA – ASOC	1.1.2024	1.1.2026	20%
BKA	Sicherheitsstandards gem. NISG im öffentl. Sektor	15.12.2020	31.12.2024	80%
BMF	Redaktioneller Ausbau der Website onlinesicherheit.gv.at	9.6.2021	31.12.2023	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	30.12.2023	55%
Regulatoren	FMA – Blackout Maturity Level Assessment	20.1.2022	31.12.2099	100%
CSP/PPP	A1 Seniorenakademie in A1 Shops	1.1.2023	31.12.2025	75%
BMI	Anpassung Cybercrime Delikte (Abstimmung mit BMJ)	31.8.2021	1.9.2023	100%

Ressort	Project	Start	Ende	Fortschritt
BMLV	Nutzung von Cyber-Threat-Intel-Plattformen zur Verdichtung des Cyber-Lagebildes	2.1.2022	1.1.2028	65%
CSP/PPP	A1 digital.campus	1.1.2020	31.12.2023	100 %
Regulatoren	FMA – Cyber Security Exercise	1.1.2022	31.12.2099	100 %
BKA	IT-Konsolidierungsprogramm: Security Framework Bund	31.3.2023	31.3.2024	85%
BMI	Cyber Cops-Bezirks IT Ermittler	31.8.2021	30.9.2025	50%
BMLV	Ausbau von Fähigkeiten zur Erkennung gezielter Manipulation des Informationsraums	1.1.2021	31.12.2031	40%
Regulatoren	RTR – Herstellerfokus	1.1.2022	31.12.2099	100 %
BMF	Forschungsprogramm Kybernet-Pass (K-PASS)	22.12.2022	30.10.2023	100 %
BKA	IT-Konsolidierungsprogramm: Security Framework Bund II – Anpassung an NIS 2	1.1.2024	31.5.2025	
CSP/PPP	A1 digital.campus - MINT & Engineering Fokus	19.2.2024	31.12.2099	10 %
BMLV	Ausbau von Fähigkeiten zur Netzwerkforensik- und Malwareanalyse sowie Reverse-Engineering	1.1.2021	30.12.2023	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	30.6.2024	80%
BKA	Erstellen eines Cyberübungsframeworks	22.11.2022	31.3.2024	90 %
BKA	Aufbau NCCA	15.12.2020	31.12.2024	75%
BMLV	Beitrag zum gesamtstaatlichen Lagebild über den Weg des IKDOK	20.3.2013	1.1.2030	100 %
CSP/PPP	FH OÖ – Fachhochschulausbildung in Informationssicherheit	31.8.2000	31.12.2099	100 %
Regulatoren	RTR – Verstärkter Fokus auf 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	1.1.2028	30%
CSP/PPP	KSÖ – Baseline Cybersecurity Standard für KMUs	27.1.2021	31.3.2023	60%
Regulatoren	RTR-Monitoring von obligatorischen 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	50%
BKA	NCC-Förderung: Cyber Security Scheck 2023	31.7.2023	31.8.2025	50%
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	50%
BMI	Erstmaßnahmen bei Cybersicherheitsvorfällen	1.7.2022	31.12.2024	30%
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	90 %
CSP/PPP	WKÖ – IT-SAFE	1.1.2022	31.12.2099	100 %
Regulatoren	RTR – Expertengruppe aus der TK-BRA	1.1.2022	1.1.2099	100 %

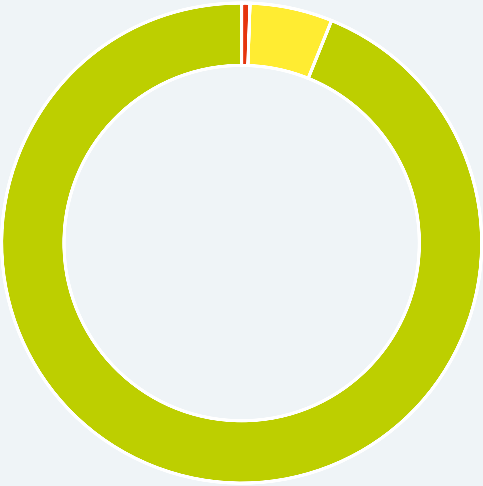
Ressort	Project	Start	Ende	Fortschritt
BMI	Schaffung einer IKT Lösung für besondere kriminalpolizeiliche Ermittlungen	18.3.2021	29.6.2025	30%
BKA	Förderung von Fortbildungsseminaren zum Thema Cyber-Gewalt in (Ex-)Paarbeziehungen	1.4.2023	31.3.2025	40%
BKA	Ausbau des Zentralen Ausweichsystem des Bundes im Rahmen der Digitalen Arche	19.11.2021	1.1.2025	40%
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	15.6.2024	20%
BKA	Einrichtung Gremium zur Technologiefolgenabschätzung	16.12.2020	31.12.2023	100%
BMLV	Fokus auf technische Entwicklungen (Digitalisierung) in der Streitkräfteplanung und -entwicklung	26.9.2017	26.9.2032	30%
Regulatoren	RTR – Vernetzung mit E-Wirtschaft	1.1.2022	31.12.2099	100%
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	55%
CSP/PPP	VERBUND – OT Cyber Security Lab	14.6.2020	31.12.2023	100%
Regulatoren	RTR – Anlassbezogene Workshops zu aktuellen Bedrohungen (z. B. SS7, FluBot/Malware, usw.)	1.1.2022	31.12.2099	100%
BMLV	Bereitstellung von OpenSource-Information durch das Cy-Dok&ForschZ (Recherche und Analyse)	1.1.2014	31.12.2024	75%
CSP/PPP	COMPARO – OPSAM Community Edition: zentrale Wissensdreh-scheibe Cybersicherheit	30.9.2021	31.12.2025	100%
BMLV	Einführung des FH-Bachelorstudiengangs „Militärische IKT-Führung“ an der TherMilAk	31.8.2022	29.6.2026	100%
CSP/PPP	DVC – TrTrainingskurs OPCYBRES: Cybersicherheit als Eckpfeiler der Unternehmensresilienz	1.11.2021	26.1.2023	100%
BMLV	Neugestaltung der ADV-Sonderverträge für IT-Personal (FF BMKÖS)	1.1.2021	31.12.2023	60%
CSP/PPP	KPMG/KSÖ-Cybersicherheitsstudie "Cybersecurity in Österreich"	30.9.2023	29.9.2024	50%
CSP/PPP	KPMG – Cyber Awareness Monat Oktober 2024: Sensibiliserung und Trainings	31.5.2024	31.12.2024	10%
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	66%
CSP/PPP	AIT – Ausbau der Cyber-Security Widerstandsfähigkeit für kritische Infrastrukturbetreiber in AT	1.1.2021	31.12.2023	90%
CSP/PPP	Learners – effizientere Methodologien + Methodiken komplexe und Dynamische Inhalte für Jugend	1.4.2022	31.12.2023	4%

Ressort	Project	Start	Ende	Fortschritt
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	1.3.2024	100 %
CSP/PPP	CSA – HackFu	30.9.2022	29.9.2023	15%
CSP/PPP	CSA – Hackerinnen Training	31.5.2023	31.12.2099	50%
CSP/PPP	SBA, sec4dev – youTube Kanal	3.9.2015	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	29.6.2025	40%
CSP/PPP	FH OÖ – CySeReS-KMU	1.1.2023	31.12.2025	2%
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	31.12.2023	90 %
CSP/PPP	AIT – Beitrag Österreichs zur Umsetzung des EU Cyber Resilience Acts	1.1.2022	31.12.2024	30%
CSP/PPP	AIT – Aufbau effektiver Threat-Intelligence Fähigkeiten für den Wirtschaftsstandort Österreich	1.1.2022	31.12.2024	40%
CSP/PPP	Mindsetters – Cyber-Awareness für Österreich – Produktname: »2b-aware«	31.7.2022	1.4.2024	98%
CSP/PPP	AKNOe -Onlinebetrug-Simulator	1.7.2021	30.6.2022	100 %
CSP/PPP	epicenter.academy: Digitale Selbstverteidigung für Lehrlinge	12.12.2022	31.12.2025	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	31.12.2024	50%
CSP/PPP	FH JOANNEUM – CSecTOR	1.12.2022	30.11.2024	20%

Auswertung für: Alle Ressorts

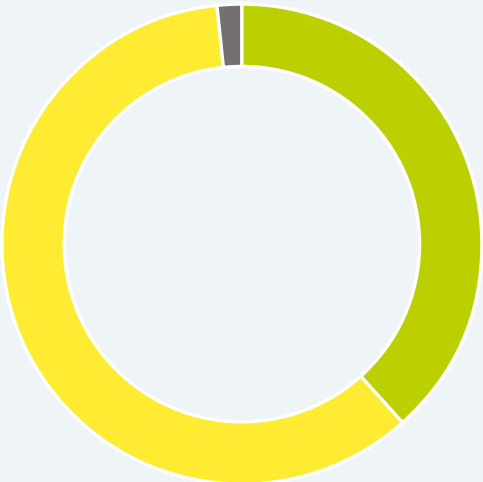
Statusindikator

- Rot: 1
- Gelb: 8
- Grün: 131



Umsetzungsstatus

- Abgeschlossen: 58
- In Arbeit: 80
- Geplant: 2



Fertigstellungsgrad

- Erfüllt: 70,52 %
- Nicht Erfüllt: 29,48 %

BKA

Projektverantwortliches Ressort
Bundeskanzleramt

Stand: 11.3.2024

Nr.	Projekt	Status	Fortschritt	Start	Ende
1	Aufbau NCC	grün	90 %	27.6.2021	31.8.2025
2	Vorantreiben Einrichtung Cyber Rapid Response Teams	gelb	20 %	21.2.2024	1.1.2099
3	Umsetzung NIS 2 Richtlinie	grün	60 %	16.1.2023	15.10.2024
4	Etablierung CISO in den Bundesministerien	grün	100 %	15.12.2020	31.12.2023
5	Ausbau des ZAS Lagezentrums zu einem IKDOK Ausweichlage-zentrum	grün	100 %	31.5.2022	31.12.2023
6	Sicherheitsstandards gem. NISG im öffentl. Sektor	grün	80 %	15.12.2020	31.12.2024
7	IT-Konsolidierungsprogramm: Security Framework Bund	grün	85 %	31.3.2023	31.3.2024
8	IT-Konsolidierungsprogramm: Security Framework Bund II – Anpassung an NIS 2	grün	0 %	1.1.2024	31.5.2025
9	Erstellen eines Cyberübungsframeworks	grün	90 %	22.11.2022	31.3.2024
10	Aufbau NCCA	grün	75 %	15.12.2020	31.12.2024
11	NCC-Förderung: Cyber Security Scheck 2023	grün	50 %	31.7.2023	31.8.2025
12	BKA – Förderungen von Projekten mit Schwerpunkt auf Bekämpfung von Cyber-Gewalt	grün	100 %	1.11.2022	31.12.2023
13	Förderung von Fortbildungsseminaren zum Thema Cyber-Gewalt in (Ex-)Paarbeziehungen	grün	40 %	1.4.2023	31.3.2025
14	Ausbau des Zentralen Ausweichsystem des Bundes im Rahmen der Digitalen Arche	grün	40 %	19.11.2021	1.1.2025
15	Erhöhung der Cybersicherheit im BKA	grün	95 %	2.11.2021	31.12.2025
16	Einrichtung Gremium zur Technologiefolgenabschätzung	grün	100 %	16.12.2020	31.12.2023

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 bis Dezember 2021 einzurichten. Die Aufgaben des NCC sind in Artikel 7 festgelegt

Wenn bis Dezember 2021 kein NCC der EK benannt wird, wird ein Vertragsverletzungsverfahren eingeleitet.

Beschreibung des Status

Optionen zur Implementierung ausgearbeitet

Entscheidung NCC im BKA aufzubauen

Umsetzung durch Trennung operative und strategische Aufgaben

Verhandlungen mit externen Dienstleister begonnen

Verhandlungen finalisiert; Vertrag unterzeichnungsreif

Vertragsabschluss mit FFG

Eingeschränkte Operativsetzung erfolgt

Aufbau interne Strukturen

Initiale Personalaufstellung abgeschlossen

Feierliche Eröffnung und Operativsetzung

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: ● gelb
Fortschritt: 20 %

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 Rechungshofprüfungen 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

Auch 2024 wurden die notwendigen Cyber Rapid Response Teams noch nicht in entsprechender Quantität/ Qualität eingerichtet.

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: Umsetzung NIS 2 Richtlinie

Start: 16.1.2023
Ende: 15.10.2024
Nr.: 5120

Aktuelles Jahr
Status: grün
Fortschritt: 60 %

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 ist 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 im Laufen.

WFA in Erstellung.

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: Ausbau des ZAS Lagezentrums zu einem IKDOK Ausweichlagezentrum

Start: 31.5.2022
Ende: 31.12.2023
Nr.: 3103

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

Gegenstand und Ziele

Der „Innerer Kreis der Operativen Koordinierungsstruktur (IKDOK)" ist eine interministerielle Struktur zur Koordination auf der operativen Ebene im Bereich der Sicherheit von Netz- und Informationssystemen bestehend aus Vertretern des Bundeskanzlers, des BMLV, des BMI und des BMEIA. Der IKDOK operiert grundsätzlich aus Wien heraus – es sind aber auch Ausweichstrukturen für Krisenfälle vorzusehen. Als Umsetzung der Ziele der ÖSCS 2021 wird im ZAS als eine zentrale Maßnahme ein Ausweichlagezentrum in St. Johann/ ZAS errichtet.

Der IKDOK muss am Standort ZAS in der Lage sein, folgende Anforderungen zu erfüllen:

•Bilden und operieren in Stabszellen (Personal, Lagebild, Einsatzführung, Versorgung, Planung, Verbindungen, Budget)

•Bilden und operieren von technischen Unterstützungselementen

•Führen des Lagebildes durch Synthese und Analyse von internen und externen Informationen

•Aufbereiten von Entscheidungsgrundlagen

•Kommunizieren mit Stakeholdern und Entscheidern

Beschreibung des Status

Anforderungsdefinition abgeschlossen

Meilensteine definiert

Verkabelungsplan erstellt

Beschaffung VKS und Synthesetool

Einrichten des Lageraums erfolgt

Einrichten der Stabszellen erfolgt

Operativer Test im Rahmen IKDOK Klausur Herbst 2023 erfolgt

Abschluss der Arbeiten

Organisationsfeld

BKA I/8

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

Internationale Zusammenarbeit

- Cyberverteidigung

- Widerstandsfähigkeit

- Cyberkriminalität und Strafverfolgung

Projekt: Sicherheitsstandards gem. NISG im öffentl. Sektor

Start: 15.12.2020
Ende: 31.12.2024
Nr.: 4

Aktuelles Jahr
Status: grün
Fortschritt: 80 %

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

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

Start: 31.3.2023
Ende: 31.3.2024
Nr.: 6124

Aktuelles Jahr
Status: grün
Fortschritt: 85 %

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

Ziel ist die Schaffung eines Zielbilds zu einem „IT Security Framework Bund« durch

- Erhebung IST – Zustand basierend auf Fragebogen

- Definition SOLL – Zustand unter Zuhilfenahme Reifegradmodell

- Konkrete Empfehlungen zur Umsetzung ausgewählter effektiver – Maßnahmen (ABER: KEINE Umsetzungsbegleitung)

Baseline Security Katalog als Grundlage gesamtstaatliche Empfehlung zu Cybersicherheitsmaßnahmen.

Beschreibung des Status

- Analyse BMEIA Vorfall 2020 Lessons Identified, Cybersicherheitsleitfaden, CISO im Bund, NIS Risikoanalyse, BSI Grundschutz, ÖISHB, NISG1, ISO27000, etc.

- Erstellung Fragebogen mit ca. 260 Fragen zu 11 Themenbereichen

- Auswahl Ministerien zur Erhebung IST-Zustand

- Erstgespräche mit CISOs der Ministerien

- Erstellung eines initialen Fragebogens zur Iststandserhebung als Grundlage zur Sollzustandsdefinition

- Erster Workshop mit IT/IT-Sec des BKA erfolgt

- Workshops mit Ministerien laufen

- Erhebungen bei Ministerien abgeschlossen

- Abschlussbericht und Empfehlungskatalog wird erstellt

Organisationsfeld

BKA I/8

Herausforderungen

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: 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: 0 %

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

Beschreibung des Status

Vorprojektphase begonnen

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: 90 %

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 im Gange

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: 31.12.2024
Nr.: 5

Aktuelles Jahr
Status: grün
Fortschritt: 75 %

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

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 Scheck 2023

Start: 31.7.2023
Ende: 31.8.2025
Nr.: 7137

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

- 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 der Richtlinie ist es, auf europäischer Ebene ein hohes gemeinsames Cybersicherheitsniveau sicherzustellen. Einen wichtigen Bestandteil dieser Sicherheitsstrategie 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 in bestimmten Sektoren, die in den Anwendungsbereich der NIS2-Richtlinie fallen, bei der Vorbereitung zur Umsetzung der dafür erforderlichen Sicherheitsmaßnahmen unterstützt. Die Finanzierung dieser Förderinitiative erfolgt zu gleichen Teilen über die Europäische Union und den Fonds Zukunft Österreich.

Beschreibung des Status

* Q3 2023: Entwicklung der Ausschreibung durch die Österreichische Forschungsförderungsgesellschaft (FFG)

* Q4 2023: Veröffentlichung der Ausschreibung durch die FFG

* Q4 2023 – Q2 2024: Ausschreibung geöffnet auf https://ecall.ffg.at/

* Q2 2024: Start der Förderung

* Q1 2025: Ende der möglichen Projektlaufzeit

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.

1. Gendersensibel – Digital -Regional

2. Digi*Strong – Empowerment von Mädchen und jungen Frauen im digitalen Raum

3. worldwideweb.amazonen – Selbstverteidigung und Selbstwirksamkeit im digitalen Raum

4. Wissen und Struktur gegen Gewalt im Web

5. EmpowerHER*

6. Let IT Dance!

7. 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: 40 %

Herausforderungen

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

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

Zielgruppe & Themenbereiche

Bewusstseinsbildung (Awareness)

- Vertrauen und Privatsphäre

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

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: 40 %

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

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

Projekt: Einrichtung Gremium zur Technologiefolgenabschätzung

Start: 16.12.2020
Ende: 31.12.2023
Nr.: 7

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

- 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

- Einrichtung eines permanenten, die Entwicklungen im Technologiesektor bewertenden Gremiums für die Gewährleistung einer systematischen Technologiebeobachtung

- Die disruptive Entwicklung der Informations- und Kommunikationstechnologie (IKT) erfordert die laufende Anpassung der Rechtsgrundlagen (Gesetze, Standards, regulatorische Vorgaben) zur Cyber-Sicherheit. Grundlage dazu ist eine systematische Technologiebeobachtung und –folgenabschätzung

Grundlage: Aus Verantwortung für Österreich. Regierungsprogramm 2020 – 2024; S.225; Durchführung hersteller- bzw. betreiberunabhängiger Technologiefolgenabschätzung bei wesentlichen

öffentlichen Digitalisierungsvorhaben sowie verstärkte Durchführung von Technologiefolgenabschätzung bei risikogeneigten Regelungsmaterien (z. B. intelligente Transportsysteme, selbstfahrende Fahrzeuge, Assistenz- und Leitsysteme etc.)

Das BMDW ist jedenfalls mit einzubeziehen

Beschreibung des Status

2021 Q2: Auftrag durch Runde der CDOs zur Bildung einer Sub-AG an BMDW ergangen

2021 Q3 Einrichtung AG Technikfolgenabschätzung unter Leitung BMDW

- Übernahme der Agenden durch BMF

Organisationsfeld

BKA

Herausforderungen

Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Ethik

- Forschung & Entwicklung

BMF

Projektverantwortliches Ressort
Bundesministerium für Finanzen

Stand: 11.3.2024

Nr.	Projekt	Status	Fortschritt	Start	Ende
1	ID Austria / E-ID	grün	100 %	30.11.2021	29.7.2022
2	oesterreich.gv.at / App Digitales Amt	grün	100 %	30.11.2021	29.4.2022
3	Ausweisplattform	grün	100 %	30.11.2021	31.12.2022
4	Redaktioneller Ausbau der Website onlinesicherheit.gv.at	grün	90 %	9.6.2021	31.12.2023
5	Forschungsprogramm Kybernet-Pass (K-PASS)	grün	100 %	22.12.2022	30.10.2023

Projekt: ID Austria / E-ID

Start: 30.11.2021
Ende: 29.7.2022
Nr.: 1012

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

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

Gegenstand und Ziele

Mit der ID Austria können sich Bürger modern, sicher und digital identifizieren. Die ID Austria ermöglicht Menschen sich sicher online auszuweisen und damit digitale Services zu nutzen und Geschäfte abzuschließen. (Quelle: https://www.oesterreich.gv.at/id-austria)

Beschreibung des Status

Digitaler Führerschein als erste Pilotanwendung ist in Betrieb

Organisationsfeld

BMF-V/B/4

Herausforderungen

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

Zielgruppe & Themenbereiche

Forschung & Entwicklung

- Internationale Zusammenarbeit

- Widerstandsfähigkeit

- Betreiber wesentlicher Dienste und kritischer Infrastrukturen

- Vertrauen und Privatsphäre

- Bildung

Projekt: oesterreich.gv.at / App Digitales Amt

Start: 30.11.2021
Ende: 29.4.2022
Nr.: 1013

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Herausforderungen
Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zugrundeliegende Strategische Ziele
Österreich kann im Zusammenwirken mit der Europäischen Union seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen

Gegenstand und Ziele
Einsatz der ID Austria und Umbau der App zur Nutzung der ID Austria Komponenten. Es sollen mit Vollbetrieb der ID Austria ausschließlich Logins über das IDA-System erfolgen.

Beschreibung des Status
Im Pilotbetrieb. Echtbetrieb ab Sommer 2022

Organisationsfeld
BMF-V/B/4

Zielgruppe & Themenbereiche
Bildung

- Vertrauen und Privatsphäre

- Betreiber wesentlicher Dienste und kritischer Infrastrukturen

- Internationale Zusammenarbeit

Projekt: Ausweisplattform

Start: 30.11.2021
Ende: 31.12.2022
Nr.: 1014

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

Gegenstand und Ziele

Einsatz der ID Austria zur Authentisierung der BenutzerInnen. Eine Nutzung der Ausweisplattform ist ausschließlich für ID Austria BenutzerInnen vorgesehen.

Beschreibung des Status

Digitaler Führerschein ist in Betrieb

Organisationsfeld

BMF-V/B/4

Herausforderungen

Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

Zielgruppe & Themenbereiche

Bildung

- Vertrauen und Privatsphäre

- Betreiber wesentlicher Dienste und kritischer Infrastrukturen

- Internationale Zusammenarbeit

Projekt: Redaktioneller Ausbau der Website onlinesicherheit.gv.at

Start: 9.6.2021
Ende: 31.12.2023
Nr.: 1016

Aktuelles Jahr
Status: grün
Fortschritt: 90 %

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
- 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 IKT-Sicherheitsportal ist eine interministerielle Initiative in Kooperation mit der österreichischen Wirtschaft und fungiert als zentrales Internetportal für Themen rund um die Sicherheit in der digitalen Welt.

Die Initiative verfolgt als strategische Maßnahme der Nationalen IKT Sicherheitsstrategie und der Österreichischen Strategie für Cyber Sicherheit das Ziel, durch Sensibilisierung und Bewusstseinsbildung der betroffenen Zielgruppen sowie durch Bereitstellung zielgruppenspezifischer Handlungsempfehlungen die IKT- und Cyber-Sicherheitskultur in Österreich zu fördern und nachhaltig zu stärken.

Durch die Redakteurinnen und Redakteure der Content-Agentur Austria (Wiener Zeitung) wird eine höhere journalistische Qualität der Inhalte erreicht. Die hohe Qualität von Fachartikeln und Experteninterviews zeichnen sich z.B. durch das Know-how bei Recherchetätigkeiten, die Themenaktualität und den professionellen Schreibstil aus.

Beschreibung des Status

Die Kooperation mit der Content-Agentur Austria läuft im Vollbetrieb, die A-SIT konsolidiert die Texte in ihrer fachlichen Kompetenz, die Abteilung V/A/3 vollzieht die endgültige Freigabe der Texte.

Monatliche Abstimmungstermine mit der Content-Agentur sowie quartalsmäßige Sitzungen mit dem Redaktionsgremium wurden/werden planmäßg eingehalten. Die Themenplanung für das Jahr 2024 ist bereits erfolgt und wurde von allen Beteiligten abgenommen.

Zusätzlich zu der laufenden Überarbeitung des Contents zur Suchmaschinenoptimierung, wurde die bessere Auffindbarkeit von themenverwandten Artikeln und Videos verstärkt. Themenzugehörige Videos sind bzw. werden laufend in die betreffenden Artikel eingebunden.

Organisationsfeld

BMF-V/A/3

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

Cyberverteidigung

- Widerstandsfähigkeit
- Bildung
- Kleine und mittlere Unternehmen (KMU)
- Wirtschaftsstandort
- Ethik
- Bewusstseinsbildung (Awareness)
- Vertrauen und Privatsphäre

Projekt: Forschungsprogramm Kybernet-Pass (K-PASS)

Start: 22.12.2022
Ende: 30.10.2023
Nr.: 7138

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Beschreibung des Status

1. Ausschreibung von Kybernet-Pass mit Budget von € 5 Mio. hat am 30. Oktober 2023 begonnen (Einreichfrist für Projektanträge: 01. März 2024)

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.

Organisationsfeld

BMF-VI/Stabsst.SiFo-TT

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

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: 11.3.2024

Nr.	Projekt	Status	Fortschritt	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: 11.3.2024

Nr.	Projekt	Status	Fortschritt	Start	Ende
1	Ausbau des Computer Security Incident Response Teams des BMI (CSIRT-BMI)	grün	100 %	31.8.2020	2.5.2023
2	Ausbau C 4 zu moderner High Tech Einheit	grün	65 %	1.1.2021	30.6.2024
3	Umsetzung und/oder funktionelle Erweiterungen der IKT-Lösungen gem. NISG	grün	45 %	1.1.2021	30.9.2027
4	ÖSCS 2021	grün	100 %	16.8.2021	29.9.2023
5	Anpassung Cybercrime Delikte (Abstimmung mit BMJ)	grün	100 %	31.8.2021	1.9.2023
6	Cyber Cops-Bezirks IT Ermittler	grün	50 %	31.8.2021	30.9.2025
7	Betrieb einer Kollaborationsplattform für den IKDOK	grün	80 %	31.8.2022	30.6.2024
8	Erlassung von Geschäftsordnungen für die Koordinierungsstrukturen	grün	100 %	31.8.2022	29.12.2023
9	Erstellung von standardisierten Vorgehensweisen (SOPs) für die Koordinierungsstrukturen	grün	50 %	1.9.2022	31.3.2024
10	Erstmaßnahmen bei Cybersicherheitsvorfällen	grün	30 %	1.7.2022	31.12.2024
11	Schaffung einer IKT Lösung für besondere kriminalpolizeiliche Ermittlungen	grün	30 %	18.3.2021	29.6.2025

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 %

Organisationsfeld
BMI

Herausforderungen
Bedrohungen, die mit der nicht sachgemäßen Nutzung von IT einhergehen

Zielgruppe & Themenbereiche
Widerstandsfähigkeit

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

Projekt: Ausbau C 4 zu moderner High Tech Einheit

Start: 1.1.2021
Ende: 30.6.2024
Nr.: 1024

Aktuelles Jahr
Status: grün
Fortschritt: 65 %

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

Cyberkriminalität und Strafverfolgung

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)

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: 45 %

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: 50 %

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 BezirksIT-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: 30.6.2024
Nr.: 3099

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 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: 50 %

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

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.

Organisationsfeld

BMI

Herausforderungen

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

Zielgruppe & Themenbereiche

Widerstandsfähigkeit

- Bewusstseinsbildung (Awareness)

- Betreiber wesentlicher Dienste und kritischer Infrastrukturen

Projekt: Erstmaßnahmen bei Cybersicherheitsvorfällen

Start: 1.7.2022
Ende: 31.12.2024
Nr.: 5121

Aktuelles Jahr
Status: grün
Fortschritt: 30 %

Zugrundeliegende Strategische Ziele

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

Gegenstand und Ziele

Erstellung eines kompletten Ausbildungskonzepts für ein einwöchiges Seminar für Erstmaßnahmen bei IT- und Cybersicherheitsvorfällen im Zuständigkeitsbereich der LVTs 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 LVTs 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.

Beschreibung des Status

Im Plan

Organisationsfeld

BMI

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: 29.6.2025
Nr.: 5122

Aktuelles Jahr
Status: grün
Fortschritt: 30 %

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: 11.3.2024

Nr.	Projekt	Status	Fortschritt	Start	Ende
1	Einrichtung von Cybercrime Kompetenzstellen an Staatsanwalt-schaften	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 %

Beschreibung des Status

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

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

Organisationsfeld

BMJ

Herausforderungen

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

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.

Zielgruppe & Themenbereiche

Cyberkriminalität und Strafverfolgung

BMLV

Projektverantwortliches Ressort
Bundesministerium für Landesverteidigung

Stand: 11.3.2024

Nr.	Projekt	Status	Fortschritt	Start	Ende
1	Ausbau und verstärkte EU-Koordinierung nationaler milCERTs (Beitrag zum CDPF-Review der EU)	rot	40 %	9.9.2021	31.12.2024
2	Erstellung eines Querschnittskonzepts »Einsatz im Cyber-Raum«	grün	100 %	3.7.2022	31.12.2023
3	Umsetzung der EU Cyber Defence Policy	grün	10 %	10.7.2023	31.12.2025
4	Durchführung von Forschungs- und Entwicklungsprojekten im nationalen und EU-Kontext	grün	55 %	23.11.2021	31.12.2032
5	Informationsgenerierung und Einbringen militärpolitischer Positionen in VN, NATO, OSZE und EU	grün	85 %	19.3.2013	31.12.2029
6	Intensivierung der internationalen Kooperation zur besseren Beitragsleistung bei Cyber-Vorfällen	grün	55 %	20.3.2013	30.12.2023
7	Nutzung von Cyber-Threat-Intel-Plattformen zur Verdichtung des Cyber-Lagebildes	grün	65 %	2.1.2022	1.1.2028
8	Ausbau von Fähigkeiten zur Erkennung gezielter Manipulation des Informationsraums	gelb	40 %	1.1.2021	31.12.2031
9	Ausbau von Fähigkeiten zur Netzwerkforensik- und Malwareanalyse sowie Reverse-Engineering	grün	70 %	1.1.2021	30.12.2023
10	Beitrag zum gesamtstaatlichen Lagebild über den Weg des IKDOK	grün	100 %	20.3.2013	1.1.2030
11	Erstellung einer Cyberverteidigungsstrategie und Fähigkeitenprofils zur Cyberververteidigung	grün	90 %	1.2.2021	31.12.2023
12	Stärkung der Cybersicherheit durch Schutz der eigenen IKT-Systeme	gelb	40 %	12.10.2020	31.12.2026
13	Fokus auf technische Entwicklungen (Digitalisierung) in der Streitkräfteplanung und -entwicklung	gelb	30 %	26.9.2017	26.9.2032
14	Verankerung der Cyber-Domäne im MSK und Aufbau von Cyber-Kräften im ÖBH	gelb	55 %	25.9.2017	26.9.2032
15	Bereitstellung von OpenSource-Information durch das CyDok&ForschZ (Recherche und Analyse)	grün	75 %	1.1.2014	31.12.2024
16	Einführung des FH-Bachelorstudiengangs „Militärische IKT-Führung“ an der TherMilAk	grün	100 %	31.8.2022	29.6.2026
17	Neugestaltung der ADV-Sonderverträge für IT-Personal (FF BMKÖS)	grün	60 %	1.1.2021	31.12.2023

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

Start: 9.9.2021
Ende: 31.12.2024
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

- Aug 2023: 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. Bisherige Aktivitäten konnten nur durch Ressourcen-Abzug aus anderen Projekten temporär wahrgenommen werden. Die AUT Mitarbeit wurde 2023 durch aktive Teilnahme an MIC und MICNET zur Erprobung und Verbesserung des Informationsaustauschs zwischen EU MilCERTs verbessert.

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

Gegenstand und Ziele

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

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

Projekt: Umsetzung der EU Cyber Defence Policy

Start: 10.7.2023
Ende: 31.12.2025
Nr.: 7129

Aktuelles Jahr
Status: grün
Fortschritt: 10 %

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

Zuständigkeiten der BMLV-Dienststellen wurden Ende 2023 eruiert, worauf der interne Umsetzungsplan erstellt wurde. Dieser wird nun regelmäßig überprüft und auf gesamtstaatlicher und EU-Ebene abgestimmt. Es bestehen mehrere Querschnitte mit anderen BMLV-Cyber-Projekten. Die Abteilung Verteidigungspolitik & Strategie ist federführend für die ressortinterne Umsetzung der Cyber Defence Policy beauftragt.

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: Durchführung von Forschungs- und Entwicklungsprojekten im nationalen und EU-Kontext

Start: 23.11.2021
Ende: 31.12.2032
Nr.: 1037

Aktuelles Jahr
Status: grün
Fortschritt: 55 %

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 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

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

Gegenstand und Ziele

Die BMLV-Verteidigungsforschung umfasst national neben der Auftragsforschung, die Teilnahme an Förderprogrammen FORTE (Verteidigungsforschungsprogramm) und KIRAS (Sicherheitsforschungsprogramm). Auf EU-Ebene steht dem BMLV der European Defence Fond (EDF), die European Defence Agency (EDA) sowie zivile EU-Förderprogramm (zB Horizon Europe) zur Verfügung.

Ziel ist, andere Maßnahmen im Cyberbereich durch gezielte F&E-Projekte bestmöglich zu unterstützen und international anschlussfähig (interoperabel) zu bleiben.

Beschreibung des Status

Das MilCyZ ist derzeit an 13 laufenden Projekten beteiligt und hat in den kommenden Jahren die Teilnahme (bzw. in einigen Projekten Federführung) an weiteren 14 Projekten geplant. Des Weiteren ist die Abteilung WFE derzeit an 24 Projekten zur Cyber-Sicherheit und -Verteidigung beteiligt: Auftragsforschung (6), FORTE (4), KIRAS (6), EDA (1), EDF (6), Digital Europe Programme (1).

Organisationsfeld

BMLV

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

Cyberverteidigung

- Widerstandsfähigkeit

- Forschung & Entwicklung

- Internationale Zusammenarbeit

- Kleine und mittlere Unternehmen (KMU)

Projekt: Informationsgenerierung und Einbringen militärpolitischer Positionen in VN, NATO, OSZE und EU

Start: 19.3.2013
Ende: 31.12.2029
Nr.: 1049

Aktuelles Jahr
Status: grün
Fortschritt: 85 %

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 BMLV ist durch die Abt. Militärpolitik sowie die Militärvertretung in Brüssel und die Militärberatung New York, Genf und Wien in diversen Foren, Arbeitsgruppen sowie Konferenzen der VN, OSZE, NATO und EU vertreten. Dadurch werden u.a. auch im Cyberbereich sowohl Informationen über aktuelle Prozesse eingeholt als auch militärpolitische Positionen nach außen vertreten.

Ziel ist es, das BMLV am aktuellen Informationsstand der Prozesse auf internationaler und EU-Ebene zu halten und militärpolitische Interessen darin zu vertreten.

In den angesprochenen Foren werden seitens MilPol insbesondere auch die Aspekte der Vertrauens- und Sicherheitsbildung sowie der Rüstungskontrolle beobachtet und bei Bedarf Beitragsleitungen geliefert.

Beschreibung des Status

Derzeitige Teilnahme an folgenden Prozessen:

VN: AUT Teilnahme an der »Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025« (OEWG II)

OSZE: AUT Teilnahme an der »IWG Cyber«

EU: AUT Teilnahme an folgenden PESCO-Projekten:

- „Cyber and Information Domain Coordination Centre (CIDCC)" (Führungsnation Deutschland) als Teilnehmer

- „Cyber Ranges Federation (CRF)" (Führungsnation Estland) als Teilnehmer

- „Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT)" (Führungsnation Litauen) als Teilnehmer

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

- Internationale Zusammenarbeit

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

Start: 20.3.2013
Ende: 30.12.2023
Nr.: 1050

Aktuelles Jahr
Status: grün
Fortschritt: 55 %

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

- Durch sich ständig ändernde Interessenslagen sowie der Rechtssituation kann auch bei intensiven Austausch und Beschaffung von Information höchstens ein Erfüllungsgrad von 80% angestrebt werden.

- Dies bedeutet eine Kenntnis der Fähigkeiten auf technologischer als auch politischer Ebene in den Interessensräumen, um in weiterer Folge eine Zuordnung (Attribuierung) oder aufgrund der beobachteten Fähigkeiten machen zu können.

- 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

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: 1.1.2028
Nr.: 1051

Aktuelles Jahr
Status: grün
Fortschritt: 65 %

Beschreibung des Status

Cyber-Threat-Intel-Plattformen sind up and running und werden aktiv im BMLV betrieben.

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.

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: gelb
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 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.

Beschreibung des Status

In diesem Segment besteht derzeit ein großes Defizit, vor allem was die Umsetzungen hinsichtlich Personals zur Planung und in weiterer Folge zu beginnender operativer Wahrnehmung betrifft, da bereits die erforderlichen Planungen an Einzelpersonen hängen. Status und Fortschritt unverändert und derzeit stagnierend.

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: 30.12.2023
Nr.: 1053

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

- 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.

- Es erfolgte kein weiterer Ausbau im Jahr 2022, sondern Erhalt der Fähigkeit 2021. Fehlende Umsetzung ist durch den Personalengpass und Rückstau des Aufwuchses begründet und daher ist aktuell keine Verstärkung der Kapazitäten möglich.

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 monatlichen 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 Cyberververteidigung

Start: 1.2.2021
Ende: 31.12.2023
Nr.: 1042

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

- 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 Cyber-Strategie der Direktion IKT & Cyber dar. Diese wird zurzeit umgesetzt.

Das BMLV beteiligt sich ebenfalls aktiv an der Umsetzung der EU Cyber Defence Policy, welche ebenfalls zur Cyber-Verteidigung Österreichs beitragen wird.

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: gelb
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

Dem Status im Jahr 2022 folgend ergaben sich hier verstärkte Verzögerungen wiederum wegen fehlender Umsetzung der Orgplan-Erweiterungen und resultierenden Problemen des Personalaufbaues. Neue Produkte, bzw. Erweiterungen zur Steigerung der Cyber-Sicherheit können nur durch Inkaufnahme von Risiken in anderen Sicherheitsbereichen temporär verkraftet werden. Dadurch kam es zum Stillstand in anderen Fähigkeitsbereichen der Cyber-Domäne. Die Auswirkungen dieser Stillstände sind temporär verkraftbar, bedeuten jedoch mittel- und langfristig keine Stärkung, sondern Verminderung des Schutzes. In der derzeitigen Prognose kann nur von Beibehaltung des aktuellen Status und auf Konzentration nur Hochrisikofaktoren ausgegangen werden.

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: gelb
Fortschritt: 30 %

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. 2024: Aufgrund des nach wie vor strukturell ungelösten Bedarfs, wurde der Status auf »Klärungsbedarf« gesetzt.

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: 🟡 gelb
Fortschritt: 55 %

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

Was den Aufbau von Cyberkräften betrifft, befinden wir uns aufgrund des weiterhin bestehenden Personalmangels derzeit erst bei einem Erfüllungsgrad von 55%. Der neue Organisationsplan sieht nun eine signifikante Aufnahme von Personal in den kommenden Jahren vor.

Der fertige Antrag seitens DionIKT&Cyber liegt seit Mitte 2023 vor und Annahme durch BMKÖS steht noch aus. Falls abgelehnt, kann dieses Ziel nicht erfüllt werden.

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: 75 %

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 akualisierte 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, zB 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: 29.6.2026
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: 31.12.2023
Nr.: 1047

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 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, Sonderfälle sind weiterhin vorhanden.

Es bleiben aber noch sehr viele offene Fragen im Praxisumgang mit den Rahmenbedingungen (z.B. eingeschränkte Mehrdienstleistungen, die längere Übungseinsätze oder Einsatzvorbereitung praktisch quasi erschweren oder durch enorme Zeiteinbussen die weitere Verwendung einschränken).

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: 11.3.2024

Nr.	Projekt	Status	Fortschritt	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	85 %	31.8.2021	30.4.2025

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 %

Beschreibung des Status

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

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

Organisationsfeld

BMEIA, II.2

Herausforderungen

Bedrohungen, die sich aus künftigen technologischen Entwicklungen ergeben

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

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.

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 Entwicklungs-projekten

Start: 31.8.2021
Ende: 30.4.2025
Nr.: 2096

Aktuelles Jahr
Status: grün
Fortschritt: 85 %

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:

- QKD4Gov – Sicherung von Behördendaten mittels Quantensicherer Kryptographie (als Konsortialpartner/Bedarfsträger)

- HYBRIS-Entwicklung einer Big Data / KI-Plattform zur Erkennung von hybriden Bedrohungen in sozialen Medien (mittels »Letter of Intent«)

Weiters Teilnahme des BMEIA am Projekt QCI-CAT (nationales AIT-Projekt im Rahmen des EuroQCI-Projekts) als »associated 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

BMAW

Projektverantwortliches Ressort
Bundesministerium für Arbeit und Wirtschaft

Stand: 11.3.2024

Nr.	Projekt	Status	Fortschritt	Start	Ende
1	[BEV] Zusätzliche Ressourcen für den Schutz der kritischen Infrastruktur	grün	0 %	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	30 %	1.12.2020	31.12.2023
4	[PRÄS] Konzept für Cybersicherheits-Berichtswesen (IKT-W)	grün	90 %	1.1.2022	31.3.2024
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	80 %	1.4.2022	31.12.2023
8	[PRÄS] Aktualisierung der IS-Richtlinie (IKT-W)	grün	90 %	30.4.2023	31.3.2024
9	[PRÄS] Überprüfung der IT-Sicherheitsmechanismen 2023 (IKT-W)	grün	100 %	1.6.2023	29.2.2024

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: 30 %

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

Ein aktuell laufendes Projekt der Sozialpartner und des BMDW befasst sich mit einer konkreten Definition auch der transversalen (digitalen) Kompetenzen und deren strukturelle Integration in die Ausbildung von Lehrberufen. Die Umsetzung erfolgt durch ibw und öibf. Es wird ein Ausgangsdokument erstellt, danach werden themenorientierte Workshops stattfinden und ein Ergebnisdokument samt Vorschlag zur Umsetzung der Ergebnisse ausgearbeitet.

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: 31.3.2024
Nr.: 4112

Aktuelles Jahr
Status: grün
Fortschritt: 90 %

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 Standardarbeitsplatz-IT-Verfahren) ist bereits eine zyklisches und sehr granulares Berichtswesen installiert.

Die Aktualisierung der IS-Richtlinie sieht eine weitere Standardisierung und Involvierung der paar verbleibenden IKT-Verfahren vor. Die Richtlinie befindet sich aktuell in Finalisierung & Review.

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-Sicherheitsmechanismen 2021 für den BMDW-Standardarbeitsplatz (IKT-W)

Start: 20.1.2023
Ende: 28.4.2022
Nr.: 4113

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

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

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.

Zielgruppe & Themenbereiche
Widerstandsfähigkeit

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.

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: 31.12.2023
Nr.: 4115

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

- 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, 215 Förderungszusagen mit einem Zuschussvolumen von rd. EUR 2,0 Mio. wurden ausgesprochen; bislang 117 ausbezahlte Zuschüsse in Höhe von rd. EUR 0,9 Mio. (Stand August 2023).

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 IS-Richtlinie (IKT-W)

Start: 30.4.2023
Ende: 31.3.2024
Nr.: 6128

Aktuelles Jahr
Status: grün
Fortschritt: 90 %

Organisationsfeld

BMAW (Präs/11)

Zugrundeliegende Strategische Ziele

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

Gegenstand und Ziele

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

Beschreibung des Status

Die generelle Überarbeitung der IS-Richtlinie ist indes bereits erfolgt und alle relevanten Anpassungsnotwendigkeiten (State-of-the-Art Vorgehen, weitreichende Governance, CISO, ISMS, Rechte & Pflichten etc.) sind enthalten.

Die Aktualisierung wurde inzwischen innerhalb der Zentralleitung sowie mit allen IKT-Vertretern der zu-/nachgeordneten Dienststellen abgestimmt und befindet sich aktuell in der finalen Review-Phase.

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-Sicherheitsmechanismen 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

BMK

Projektverantwortliches Ressort
Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie

Stand: 11.3.2024

BMKOES

Projektverantwortliches Ressort
Ministerium für Kunst, Kultur, öffentlichen Dienst und Sport

Stand: 11.3.2024

BMSGPK

Projektverantwortliches Ressort
Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz

Stand: 11.3.2024

Nr.	Projekt	Status	Fortschritt	Start	Ende
1	IT-System zur Erkennung von sicherheitskritischen Ereignissen (SIEM) gemäß Etappenplan	grün	80 %	1.2.2023	15.12.2024
2	Etablierung Leitlinien Risikomgmt. in der Netz- und Informationssicherheit	grün	80 %	1.2.2023	30.9.2024
3	Weiterentwicklung des Informationssicherheitsmanagement (ISMS) Tools	grün	70 %	1.2.2023	31.12.2024
4	Erstellung eines Maßnahmenplans zur Netz- und Informationssicherheit	grün	30 %	1.1.2024	30.9.2024

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

Start: 1.2.2023
Ende: 15.12.2024
Nr.: 6120

Aktuelles Jahr
Status: grün
Fortschritt: 80 %

Organisationsfeld
BMSGPK I/B/8

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 Dateschutzanforderungen.

Status 15.05.2023: Freigabe zum Einsatz des SIEM-Systems an den IT Service Provider erfolgt. Die ersten 6 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 einem SOC liegt vor.

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: 30.9.2024
Nr.: 6121

Aktuelles Jahr
Status: grün
Fortschritt: 80 %

Status 26.02.2024:
Toolentscheidung hinsichtlich BMF Reporting Plattform getroffen, Prozess zur Risikoerhebung 2024 gestartet

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.

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: 31.12.2024
Nr.: 6122

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 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 montalichen 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. 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: 30.9.2024
Nr.: 8153

Aktuelles Jahr
Status: grün
Fortschritt: 30 %

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.

Beschreibung des Status

02.01.2024: Festlegung des Projektteams und des zu betrachtenden Scopes

18.01.2024: Erstellung und Freigabe des Projektauftrages

01.02.2024: Inkraftsetzung einer Grobkostenstruktur sowie einer zentralen Datei- und Dokumentenablage

15.02.2024: Identifizierung erster Prüfmechanismen und -maßnahmen für die Errichtung einer vollumfänglichen GAP-Analyse

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: 11.3.2024

Nr.	Projekt	Status	Fortschritt	Start	Ende
1	A1 Seniorenakademie	grün	100 %	31.3.2021	31.12.2023
2	Uni Wien – DaTra	grün	100 %	1.12.2022	31.1.2024
3	SBA – ASOC	grün	20 %	1.1.2024	1.1.2026
4	A1 Seniorenakademie in A1 Shops	grün	75 %	1.1.2023	31.12.2025
5	A1 digital.campus	grün	100 %	1.1.2020	31.12.2023
6	A1 digital.campus – MINT & Engineering Fokus	grün	10 %	19.2.2024	31.12.2099
7	FMA,OENB – TIBER AT Framework	grün	100 %	6.4.2021	31.12.2023
8	FMA, OeNB – Threat Led Penetration Testing	grün	30 %	1.1.2023	1.1.2028
9	KSÖ – Baseline Cybersecurity Standard für KMUs	grün	60 %	27.1.2021	31.3.2023
10	FH OÖ – Fachhochschulausbildung in Informationssicherheit	grün	100 %	31.8.2000	31.12.2099
11	WKÖ – IT-SAFE	grün	100 %	1.1.2022	31.12.2099
12	WKÖ – CYBER SECURITY HOTLINE WKO	grün	100 %	1.1.2022	31.12.2099
13	WKÖ – CYBER SECURITY FEUERWEHR WKO	gelb	20 %	1.1.2022	31.12.2099
14	WKÖ – Women4Cyber Austria	grün	100 %	31.8.2022	31.12.2099
15	VERBUND – OT Cyber Security Lab	grün	100 %	14.6.2020	31.12.2023
16	COMPARO – OPSAM Community Edition: zentrale Wissensdrehscheibe Cybersicherheit	grün	100 %	30.9.2021	31.12.2025
17	DVC – TrTrainingskurs OPCYBRES: Cybersicherheit als Eckpfeiler der Unternehmensresilienz	grün	100 %	1.11.2021	26.1.2023
18	KPMG/KSÖ-Cybersicherheitsstudie »Cybersecurity in Österreich«	grün	50 %	30.9.2023	29.9.2024
19	KPMG – Cyber Awareness Monat Oktober 2024: Sensibiliserung und Trainings	grün	10 %	31.5.2024	31.12.2024
20	INDUCE Cyber Security Literacy And Dexterity through Cyber Exercises	grün	30 %	1.4.2021	31.3.2024
21	AIT – Post-Quanten-Computer sichere Verschlüsselung für höchste Cyber Sicherheit	grün	66 %	1.1.2021	31.12.2026
22	AIT – Ausbau der Cyber-Security Widerstandsfähigkeit für kritische Infrastrukturbetreiber in AT	grün	90 %	1.1.2021	31.12.2023
23	Learners – effizientere Methodologien + Methodiken komplexe und Dynamische Inhalte für Jugend	gelb	4 %	1.4.2022	31.12.2023
24	Nationales Cyber Security Trainingszentrum	gelb	2 %	31.8.2022	31.12.2025

Nr.	Projekt	Status	Fortschritt	Start	Ende
25	VISP – Vienna InternetSecurityPrivacy Cluster	grün	100 %	1.3.2020	31.12.2099
26	OCG – Young Researchers Day	grün	100 %	1.3.2024	1.3.2024
27	CSA – HackFu	grün	15 %	30.9.2022	29.9.2023
30	CSA – Hackerinnen TrainingVISP – Vienna InternetSecurityPrivacy Cluster	grün	50 %	31.5.2023	31.12.2099
29	SBA, sec4dev – youTube Kanal	grün	grün	3.9.2015	31.12.2099
30	SBA, ÖIAT – Security Awareness Stammtisch	grün	grün	24.4.2023	31.12.2099
31	SBA – Cybersecurity Quiz	grün	grün	30.9.2021	31.12.2099
32	SBA – securepizza.club @ SBA Research	grün	100 %	1.1.2021	31.12.2099
33	SBA – Women in Privacy & Security Vienna	grün	100 %	1.1.2021	31.12.2099
34	SBA – Seurity Meetup	grün	100 %	1.1.2021	31.12.2099
35	ISPA – Der Online-Zoo	grün	75 %	1.12.2015	1.7.2025
36	ACSC – Austrian Cyber Security Challenge 2023	grün	60 %	1.1.2023	31.12.2023
37	ECSC – European Cyber Security Challenge 2023	grün	50 %	1.1.2023	31.12.2023
38	openECSC – Open European Cyber Security Challenge 2023	grün	35 %	20.1.2023	31.12.2023
39	FH OÖ – SSCCS (Secure Supply Chains for critical systems)	grün	40 %	30.6.2021	29.6.2025
40	FH OÖ – CySeReS-KMU	grün	2 %	1.1.2023	31.12.2025
41	FH OÖ – Sucredi	grün	100 %	1.1.2019	29.6.2022
42	AIT -Aufbau von Übungs- und Trainingsplattformen für Multistakeholder Infrastrukturszenarien	grün	70 %	30.9.2022	31.12.2024
43	AIT – Realisierung von Cyber Security Schlüsseltechnologien made in Austria mit globalem Impact	grün	90 %	1.1.2022	31.12.2023
44	AIT – Beitrag Österreichs zur Umsetzung des EU Cyber Resilience Acts	grün	30 %	1.1.2022	31.12.2024
45	AIT – Aufbau effektiver Threat-Intelligence Fähigkeiten für den Wirtschaftsstandort Österreich	grün	40 %	1.1.2022	31.12.2024
46	Mindsetters – Cyber-Awareness für Österreich – Produktname: »2b-aware«	grün	98 %	31.7.2022	1.4.2024
47	AKNOe -Onlinebetrug-Simulator	grün	100 %	1.7.2021	30.6.2022
48	epicenter.academy: Digitale Selbstverteidigung für Lehrlinge	grün	50 %	12.12.2022	31.12.2025
49	AIT – Österreich als aktiver EU Cyber Security Skill Development Stakeholder	grün	10 %	1.6.2023	31.12.2026
50	SV – Weiterentwicklung SV-Sicherheitsstandards	grün	80 %	1.10.2022	31.3.2024
51	FH JOANNEUM – Masterstudium IT & Mobile Security	grün	100 %	1.1.2001	31.12.2099
52	FH JOANNEUM – CyMoDACS: Cyber-Security and Mobility for Digital Aeronautic Communication Systems	grün	50 %	1.1.2022	31.12.2024
53	FH JOANNEUM – CSecTOR	grün	20 %	1.12.2022	30.11.2024

Projekt: A1 Seniorenakademie

Start: 31.3.2021
Ende: 31.12.2023
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: Uni Wien – DaTra

Start: 1.12.2022
Ende: 31.1.2024
Nr.: 8159

Aktuelles Jahr
Status: grün
Fortschritt: 100 %

Organisationsfeld
Universität Wien, Fakultät für Informatik, Forschungsgruppe Security & Privacy

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/

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: 20 %

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: A1 Seniorenakademie in A1 Shops

Start: 1.1.2023
Ende: 31.12.2025
Nr.: 7150

Aktuelles Jahr
Status: grün
Fortschritt: 75 %

Zugrundeliegende Strategische Ziele

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

Gegenstand und Ziele

Seit 2023 finden in ausgewählten A1 Shops in Wien, Linz, Salzburg, Graz und Innsbruck wöchentlich kostenlose Schulungen für die Generation 60+ statt. A1 GURUS informieren zu Tipps&Tricks für die optimale und sichere Nutzung des eigenen 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: 31.12.2023
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: 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: 1.1.2028
Nr.: 8148

Aktuelles Jahr
Status: grün
Fortschritt: 30 %

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 Resiliance Act (DORA) wird künftig ausgewählte Finanzunternehmen zur Durchführung von Threat Led Penetration Tests (TLPT) verpflichten. In Vorbereitung darauf haben die Finanzmarktaufsicht (FMA) und die Oesterreichische Nationalbank (OeNB) gemeinsam die Eckpunkte für die Durchführung derartiger Tests in Österreich entwickelt (TIBER-AT -Implementation Guide). Im Jahr 2024 findet eine Pilotphase statt. Zudem wird die Ausgestaltung von TLPT unter DORA in Zusammenarbeit mit internationalen Institutionen weiter konkretisiert (Arbeitsteilung mit der EZB-Bankenaufsicht, Mitarbeit in Arbeitsgruppen zu begleitenden Regularien). Ab 2025 werden Finanzunternehmen, die unter den TLPT-Scope von DORA fallen, unter Begleitung von OeNB und FMA tourlich TLPT-Tests durchführen. Ziel des Projektes ist die Schaffung der entsprechenden Voraussetzungen sowie die Sicherstellung der fortlaufenden Testbetreuung.

Beschreibung des Status

‹- 2023: Erstellung TIBER-Implementation Guide; Workshops mit Finanzunternehmen; Gründung TIBER Cyber Team Österreich (TCT-AT) in der OeNB

- 2024: Durchführung Pilotphase, Konkretisierung der weiteren Ausgestaltung in Zusammenarbeit mit internationalen Institutionen (Arbeitsteilung mit SSM für Significant Institutions, Mitarbeit in Arbeitsgruppen am RTS on TLPT der ESAs).

- Ab 2025: Tourliche TLPT-Tests für Finanzunternehmen, die unter den TLPT-Scope von DORA fallen; Begleitung durch OeNB und FMA

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

- 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 %

Organisationsfeld

Bundessparte Information und Consulting/Wirtschaftskammer Österreich

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

Women4Cyber Austria ist eine Initiative mit dem Ziel, Frauen im Bereich der Cybersicherheit zu fördern, zu ermutigen und zu unterstützen und das Bewusstsein für eine gender-inklusive Cybersicherheits-Community zu erhöhen. Es handelt sich um das österreichische Chapter der europäischen Non-Profit-Organisation Women4Cyber.

Beschreibung des Status

fortlaufende Aktivitäten

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 von VERBUND wurde im Jahr 2020 gegründet und es wird seither aufgebaut. Den zentralen Angelpunkt des Labors stellt eine Testumgebung dar, in der neue Systeme der OT (Operational Technology) bereitgestellt und Prozesse aus dem Kraftwerksbetrieb realitätsnah abgebildet werden. Die Systeme werden anschließend Cyber Security Prüfungen (Penetration Tests) unterzogen und gemeinsam mit externen Partnern und Forschungseinrichtungen werden neue Methoden zur Absicherung der OT Infrastruktur entwickelt und 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.

Beschreibung des Status

- Erweiterung u. physischer Ausbau des OT Cyber Security Labs

– Das Projekt wurde Ende 2023 abgeschlossen

Ab 2024 wird das OT Cyber Security Lab regulär als Teil der Abteilung Infomationssicherheit 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 – TrTrainingskurs OPCYBRES: Cybersicherheit als Eckpfeiler der Unternehmensresilienz

Start: 1.11.2021
Ende: 26.1.2023
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: Freier Kurs Zugang https://doktorb.mymemberspot.de/auth/register

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: 30.9.2023
Ende: 29.9.2024
Nr.: 2071

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

- 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 (KPMG Security Services GmbH) veröffentlicht jährlich in Zusammenarbeit mit dem Sicherheitsforum Digitale Wirtschaft des Kompetenzzentrums Sicheres Österreich (KSÖ) die Cyber Security Studie für Österreich. Diese Studie, an der 2022 ~550 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 7. Ausgabe der Cyber Security Studie für das Jahr 2022 abgeschlossen und am 4. Mai 2022 im Raiffeisenforum präsentiert.

Die Planungen und Aufbereitungen der Inhalte für die 8. Ausgabe laufen bereits. Diese soll voraussichtlich im Mai 2023 veröffentlicht und präsentiert.

‹-Die 8. Ausgabe der Cyber Security Studie für das Jahr 2023 abgeschlossen und wurde am 4. Mai 2022 im Haus der Industrie (IV) -Die Planungen für die 9. Ausgabe laufen bereits. Diese wurde im Mai 2023 veröffentlicht und präsentiert.

‹-Die 9. Ausgabe der Cyber Security Studie für das Jahr 2024 ist in Durchführung und wird voraussichtlich im Q2 2024 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: Sensibiliserung und Trainings

Start: 31.5.2024
Ende: 31.12.2024
Nr.: 7149

Aktuelles Jahr
Status: grün
Fortschritt: 10 %

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 Mögiichenkeiten, 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: 66 %

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.);

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: 31.12.2023
Nr.: 2074

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 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 Infrastrukturbettreiber 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. Österreich hat sich als international führendes Kompetenzzentrum im Bereich Cyber Securit etabliert – das AIT ist das erste und derzeit einzige offizielle „Collaboration Center" der IAEA zum Thema Cyber Security. In dieser Rolle werden Cyber Security Trainings für kritische Infrastrukturbetreiber weltweit durchgeführt -https://www.iaea.org/newscenter/news/ait-austrian-institute-of-technology-becomes-the-first-iaea-collaborating-centre-for-information-and-computer-security-for-nuclear-security).

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

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 %

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

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

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: 1.3.2024
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 und vom OCG Arbeitskreis IT-Sicherung und dem FFG COMET Kompetenzzentrum SBA-K1 organisiert. Jungforschende können im Zuge der IKT ihre Forschung vorstellen. Ziel ist 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

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: CSA – Hackerinnen Training

Start: 31.5.2023
Ende: 31.12.2099
Nr.: 8155

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

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

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, regelmäßige 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.

Beschreibung des Status

- monatliche Trainings

- Erweiterung des TrainerInnen Pools

- Community Building

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

Organisationsfeld

CSA – CyberSecurityAustria

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: 3.9.2015
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 eines der wichtigsten Erfolgskriterien für mehr IT-Sicherheit in Unternehmen. In einem informellen und vertrauensvollen Rahmen wollen wir 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 Algorithemn und Küstliche Intelligenz. In 13 Themen sind die Inhalte kurz, spielerisch & interaktiv aufgearbeitet. 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

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

Der Club soll als Plattform für Studierende und als Treffpunkt dienen. Ein Ort, an dem man sich zu aktuellen Sicherheitsthemen ua 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

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

Forschung & Entwicklung

- 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 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

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

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

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

Bildung

- Forschung & Entwicklung

Projekt: SBA – Security 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 bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

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)

- Wirtschaftsstandort

- Kleine und mittlere Unternehmen (KMU)

- Betreiber wesentlicher Dienste und kritischer Infrastrukturen

- 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 urkainische, 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 %

Organisationsfeld

CSA – CyberSecurityAustria

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.

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 wärend des ECSC2023 Finales in Hamar gespielt.

Dies ist vor allem für die SecurityExperten vieler Unternehmen weltweit eine willkommen 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 zweitenmal ausgetragen und soll ab 2023 als fixer Bestandteil Europäischer Exzellenz-/Nachwuchsarbeit ebenso positioniert werden wie als Europäischer Leuchturm 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: 29.6.2025
Nr.: 4116

Aktuelles Jahr
Status: grün
Fortschritt: 40 %

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 (FFG Coin FH4Wirtschaft) zum Thema Supply Chain Cyber Security mit FH St. Pölten (Cyber Security Department). Im Projekt werden ua Supply Chains von fünf Use Case Partnern nach Cyber Security und Resilienz-Aspekten analysiert

Beschreibung des Status

‹- Projekt gestartet

- Use Cases gestartet (Industrie, Logistik, Lebensmittelbereich)

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: 31.12.2025
Nr.: 4117

Aktuelles Jahr
Status: 🟢 grün
Fortschritt: 2 %

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 analyisierte vier Supply Chains österreichischer Unternehmen. Output des Projektes ist ua. 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: 31.12.2023
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: 31.12.2024
Nr.: 4122

Aktuelles Jahr
Status: grün
Fortschritt: 30 %

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

Cyber Security by Design Produktentwicklungsmethoden und Werkzeuge für neue IoT Märkte durch „made in Austria" Technologie am AIT in Entwicklung

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: 31.12.2024
Nr.: 4123

Aktuelles Jahr
Status: grün
Fortschritt: 40 %

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

Erster Prototyp für die NIS Behörde durch AIT 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: 1.4.2024
Nr.: 6123

Aktuelles Jahr
Status: ● grün
Fortschritt: 98 %

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: Plannungsbeginn

- Dezember 2022: Definition der Anforderungen und technische Plannung

- 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

- 1.April: 2024: Go-Live 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 für Lehrlinge

Start: 12.12.2022
Ende: 31.12.2025
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 bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Nachfrage des Arbeitsmarktes zu erfüllen

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-Trainersprogramm 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) ergänzt das Angebot. Die Inhalte sind in neun Kapitel gegliedert und behandeln digitale Verschlüsselung, sichere Kommunikation, den Umgang mit Passwörtern,Phishing, die Gründe für Datenschutz und digitale Selbstverteidigung und mehr. 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 November 2022 haben wir in über 110 Workshops rund 2.500 Schüler:innen in unterschiedlichen Standorten in Niederösterreich und Wien erreicht. 2024 können wir durch eine Förderung vom Land auch für Jugendliche in der Steiermark kostenlose Workshops anbieten. Unser offenes E-Learning wird außerdem vom BMBWF über die Eduthek.at auch für die Anwendung in der Oberstufe und die Fortbildung von Lehrkräften empfohlen. Das frei zugängliche E-Learning wird, unterstützt durch eine Netidee Förderung, weiter ausgebaut.

Organisationsfeld

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

Zielgruppe & Themenbereiche

Bildung

- Kleine und mittlere Unternehmen (KMU)

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 Koordinierungstelle 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 %

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:

Master: IT & Mobile Security – Berufsbegleitende

Master: IT-Recht & Management – Berufsbegleitend

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

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: 31.12.2024
Nr.: 7134

Aktuelles Jahr
Status: grün
Fortschritt: 50 %

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: 20 %

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

laufend

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: 11.3.2024

Nr.	Projekt	Status	Fortschritt	Start	Ende
1	E-Control Energie-Branchenrisikoanalyse	grün	10 %	1.1.2024	31.3.2025
2	FMA – Assessment der Mitigationsmaßnahmen	grün	100 %	1.1.2024	31.12.2099
3	FMA – DORA-Gap-Analyse	grün	20 %	1.1.2024	31.12.2099
4	FMA – DORA-Implementierung	grün	20 %	8.2.2024	31.12.2025
5	FMA – IT Governance Deep Dives	grün	50 %	30.9.2023	31.12.2099
6	FMA – Cyber Maturity Level Assessment	grün	100 %	1.1.2022	31.12.2099
7	FMA – Vor-Ort-Prüfungen bei den beaufsichtigten Finanzunternehmen	grün	100 %	30.6.2018	31.12.2099
8	FMA – Blackout Maturity Level Assessment	grün	100 %	20.1.2022	31.12.2099
9	FMA – Cyber Security Exercise	grün	100 %	1.1.2022	31.12.2099
10	RTR – Herstellerfokus	grün	100 %	1.1.2022	31.12.2099
11	RTR – Verstärkter Fokus auf 5G-Sicherheit	grün	100 %	1.1.2022	15.6.2022
12	RTR -Monitoring von obligatorischen Informationssicherheitsmanagement und Sicherheitsstandards	grün	100 %	1.1.2022	15.6.2022
13	RTR – TK-Branchenrisikoanalyse (TK-BRA)	grün	50 %	1.1.2022	15.6.2022
14	RTR – Expertengruppe aus der TK-BRA	grün	100 %	1.1.2022	1.1.2099
15	RTR – Behördentreffen IT-Risiko	grün	100 %	1.1.2022	31.12.2099
16	RTR – Mustersicherheitskonzept	grün	20 %	1.1.2022	15.6.2024
17	RTR – Vernetzung mit E-Wirtschaft	grün	100 %	1.1.2022	31.12.2099
18	RTR – Anlassbezogene Workshops zu aktuellen Bedrohungen (z.B. SS7, FluBot/Malware, usw.)	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: 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

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, Sektorenverteter 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).

Beschreibung des Status

für 2022 abgeschlossen;

nächste Aktualisierung 2024/25 Beginn 2024, Fertigstellung 2025

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

- 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: 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

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: 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

- 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 struktrierten 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 (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-Implementierung

Start: 8.2.2024
Ende: 31.12.2025
Nr.: 8151

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

- 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

Ab 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, die beaufsichtigten Unternehmen bei der Umsetzung von DORA zu unterstützen sowie FMA-intern die Erfüllung der neuen Aufsichtsaufgaben bereichsübergreifend zu koordinieren:

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. Koordinierung des DORA-Vollzugs iSd integrierten Aufsichtsansatzes

4. Externe Kommunikationsmaßnahmen sowie FMA-interner Wissenstransfer

Beschreibung des Status

‹- Einbezug von DORA-Aufsichtsaufgaben in die strategische Planung und Steuerung

- Schaffung organisatorischer Grundlagen zur koordinierten DORA-Umsetzung

- FMA-Vertretung von abgestimmten Positionen zu DORA in nationalen und europäischen Gremien

- Vorbereitungen zur Koordinierung des DORA-Vollzugs

- 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 Deep Dives

Start: 30.9.2023
Ende: 31.12.2099
Nr.: 8152

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 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-Deep-Dives 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

‹- Pilotprojekt an ausgewähltem Institut

- Ausrollung auf weitere LSI

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 Maturity Level Assessment

Start: 1.1.2022
Ende: 31.12.2099
Nr.: 4106

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

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 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

‹- Entwicklung und Durchführung bei ausgewählten Versicherungsunternehmen 2022

- Ableitung von Handlungsempfehlungen und Rückmeldungen an die beaufsichtigten Unternehmen in Feedbackgesprächen

- Durchführung mit weiteren Versicherungsunternehmen (seit 2023)

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 – 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, indem ihre Kontrollumgebungen an internationale Standards angenähert werden.

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

- Plan: 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: 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

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 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

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: 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

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)

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 – Herstellerfokus

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 wird sich im Laufe des Jahres 2022 konstituieren und dient dem zuständigen Bundesministerium als zum einen als Beratungsgremium und zum anderen als Expertengremium zur Erstellung von Gutachten im Zuge der Einstufung eines Herstellers als «Hochrisikolieferant». Die RTR übernimmt 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 – Verstärkter Fokus auf 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 Rollout von 5G-Mobilfunknetzen steht für eine neue Generation im Mobilfunk, die eine breite Palette an innovationen Anwendungen bringen soll. Damit verknüpft sind erhöhte Anforderungen an die Sicherheit der 5G-Netze und 5G-Dienste. Der Maßnahmenkatalog der europäischen 5G Cybersecurity Toolbox trägt dem 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 -Monitoring von obligatorischen Informationssicherheitsmanagement und Sicherheits-standards

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 nunmehr 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: 50 %

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 leitet Maßnahmenempfehlungen für die Stakeholder ab. Eine Aktualisierung findet im Abstand von 2-3 Jahren statt. Derzeit finden Aktivitäten zur Aktualisierung der Branchenrisikoanalyse statt, der Abschluss ist für Q1/2024 geplant.

Beschreibung des Status

‹- Aktuell finden Aktivitäten zur Aktualisierung der Branchenrisikoanalyse statt

- Abschluss der Branchenrisikoanalyse 2023 ist für Q1/2024 geplant

https://www.rtr.at/TKP/was_wir_tun/telekommunikation/anbieterservice/netzsicherheit/Risikoanalysen.de.html

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 – Expertengruppe aus der TK-BRA

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

laufend

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: 15.6.2024
Nr.: 2105

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

- 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 im Jahr 2024 gemeinsam mit ISPA

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

Ein Ergebnis der bisherigen TK-Branchenrisikoanalysen betrifft die Herausforderung gegenseitiger Abhängigkeiten von TK- und Energiebranche. Um gemeinsame Risiken sowie Kaskadeneffekte zu identifizieren haben RTR und Vertreter der E-Wirtschaft eine Vernetzung hergestellt, die sich regelmäßig mit den 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

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