Bundeskanzleramt

Bundesministerium
Inneres

Bundesamt für Verfassungsschutz
und Terrorismusbekämpfung

Mapping-Tabelle von IKT-Sicherheitsstandards und Cyber Security Best Practices

NIS Fact Sheet 8/2018

Wien, März 2020

Inhalt

1 Einleitung 3

2 NIS-Kooperationsgruppe 4

2.1 Reference document on security measures for OES 4

2.2 Mapping internationaler Informationssicherheitsstandards 4

3 Versionshistorie 17

Impressum 18

1 Einleitung

Nach der **Richtlinie (EU) 2016/1148** des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union („**NIS-Richtlinie**“) müssen in Österreich bestimmte öffentliche und private Einrichtungen Maßnahmen ergreifen, um die Risiken für die Sicherheit ihrer Netz- und Informationssysteme zu bewältigen und den Auswirkungen von Sicherheitsvorfällen vorzubeugen bzw. diese so gering wie möglich zu halten.

Österreich setzt die NIS-Richtlinie mit dem am 28. Dezember 2018 kundgemachten Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (**Netz- und Informationssystemsicherheitsgesetz** – **NISG**) um. Mit der Verordnung zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (**Netz- und Informationssystemsicherheitsverordnung** – **NISV**) wurden **Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste** festgelegt.

Um die Betreiber wesentlicher Dienste im Sinne der guten Kooperation bei der Umsetzung der Vorgaben aus dem NISG und der NISV zu unterstützen, wird in diesem **NIS Fact Sheet** eine „**Mapping-Tabelle**“, das heißt eine Gegenüberstellung der Sicherheitsmaßnahmen mit bestehenden nationalen und internationalen IKT-Sicherheitsstandards wie auch Cyber Security Best Practices, zur Verfügung gestellt.

Dieses Dokument kann als Grundlage für die Erarbeitung **sektorenspezifischer Sicherheitsvorkehrungen** bzw. Sicherheitsstandards herangezogen werden. Eine nähere Erläuterung der in der NISV genannten Sicherheitsmaßnahmen findet sich im **NIS Fact Sheet 8/2019** „Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste“. Es sei darauf hingewiesen, dass Änderungen vorbehalten sind.

2 NIS-Kooperationsgruppe

Um den Austausch zwischen den EU-Mitgliedstaaten im Bereich der Sicherheit von Netz- und Informationssystemen zu unterstützen, die strategische Zusammenarbeit zu erleichtern und die Entwicklung von Grundsätzen für die europäische Zusammenarbeit bei Cyberkrisen zu fördern, wurde eine Kooperationsgruppe aus Vertretern der Mitgliedstaaten, der Europäischen Kommission und der Agentur der Europäischen Union für Cybersicherheit (ENISA) eingerichtet (**„NIS-Kooperationsgruppe“**).

2.1 Reference document on security measures for OES

Im Rahmen der Kooperationsgruppe werden in Work Streams Leitfäden und Referenzdokumente zu diversen informationssicherheitsrelevanten Themenbereichen erarbeitet. In dem Work Stream „Security measures for Operators of Essential Services (OES)“ haben Mitgliedstaaten mit Unterstützung von ENISA einen Leitfaden für Betreiber wesentlicher Dienste erstellt, welcher als Grundlage zur Unterstützung für die Absicherung wesentlicher Dienste freiwillig verwendet werden kann. Dieses Referenzdokument ist auf der Homepage der Kooperationsgruppe zum Download verfügbar.[1]

2.2 Mapping internationaler Informationssicherheitsstandards

Die NIS-Richtlinie gibt vor, dass die Mitgliedstaaten bei der Umsetzung die Anwendung europäischer oder international anerkannter Normen und Spezifikationen für die Sicherheit von Netz- und Informationssystemen zu fördern haben, um eine einheitliche Anwendung der Richtlinie zu gewährleisten.[2] Auf Basis dessen wurde innerhalb des Work Streams „Security measures for Operators of Essential Services (OES)“ eine Grundlage für ein Mapping erarbeitet und für die Mitgliedstaaten zur Verfügung gestellt. Dieses Mapping wurde mit nationalen Informationssicherheitsstandards erweitert und ist in Anlehnung an die Sicherheitsmaßnahmen des „Reference document on security measures for OES“ in vier Bereiche unterteilt:

- Teil 1: Governance und Ökosystem
- Teil 2: Schutz

[1] CG Publication 01/2018 - Reference document on security measures for Operators of Essential Services, abrufbar unter https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

[2] Vgl. Art. 19 NIS-Richtlinie.

- Teil 3: Verteidigung
- Teil 4: Resilienz

Auf den folgenden Seiten findet sich die Gegenüberstellung der Sicherheitsmaßnahmen aus der NISV, die auf die im Referenzdokument ersichtlichen Mindestsicherheitsmaßnahmen zurückgehen, mit nationalen und internationalen IKT-Sicherheitsstandards wie auch Cyber Security Best Practices (Mapping).

2.2.1 Governance und Ökosystem

#	Kategorie	Sicherheitsmaß-nahme	Ö. Informations-sicherheitshandbuch Version 4.0.1	BSI IT-Grund-schutz[3]	ISO 27001:2013	ISA/IEC 62443 3-3	ISA/IEC 62443 2-1	CIS CSC Version 7.0	NIST CYBER SECURITY FRAME-WORK	ÖNORM A7700-4
1	Governance und Risikomanage-ment	Risikoanalyse	4 Risikoanalyse	BSI-Standard 100-2, Kapitel 3, 4, 5, BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz	8.2 Information security risk assessment 8.3 Information security risk treatment	-	ORG 2.1	1, 2, 3, 13, 14, 17	ID.GV-4 ID.RA-1,2,3,4,5,6 ID.RM-1,2,3 PR.AT-2	-
		Sicherheitsrichtlinie	5 Informations-si-cherheitspolitik	BSI-Standard 100-2, Kapitel 3.1, B 1.0, B 1.16, B 1.5, M 2.10, M 2.163, M 2.205, M 2.217,M 2.336, M 2.337, M 2.340, M 2.550, M 3.2, M 4.99	A.5.1 Management direc-tion for information secu-rity A 18.1 Compliance with le-gal and contractual re-quirements A.6.1.5 Information secu-rity in project manage-ment	-	ORG 1.1, 2.3, DATA 1.1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20	ID.GV-1,2,3	-
		Überprüfungsplan der Netz- und Infor-mationssysteme	2.3 Umsetzung des Informations-sicher-heitsplans	M 2.64, M 2.199, M 4.81	A.12.7.1 Information sys-tems audit controls	-	ORG 2.2, CM 1.3	3	-	-
		Ressourcen-ma-nagement	-	M 2.214	A.12.1.3.Capacity Ma-nagement	-	AVAIL 1.2	3, 6	-	-

[3] Hinweis: Die BSI-Standards 200-1, 200-2 und 200-3 lösen seit Oktober 2017 die BSI-Standards der Reihe 100-x ab. Den IT-Grundschutz-Anwendern stellt das BSI zur erfolgreichen Migration eine „Anleitung zur Migration von Sicherheitskonzepten“ zur Verfügung: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/Migrationsleitfaden/Anleitung_zur_Migration.html

#	Kategorie	Sicherheitsmaß-nahme	Ö. Informations-sicherheitshandbuch Version 4.0.1	BSI IT-Grund-schutz[3]	ISO 27001:2013	ISA/IEC 62443 3-3	ISA/IEC 62443 2-1	CIS CSC Version 7.0	NIST CYBER SECURITY FRAME-WORK	ÖNORM A7700-4
		Informations-sicher-heits-management-systemprüfung	3.3 Interne ISMS Audits 18 Security Compli-ance	BSI-Standard 100-2, Kapitel 6.1.1 M 2.199	9.2 Internal Audit	-	ORG 2.4	1, 2, 3, 6, 17	PR.PT-1	5
		Personalwesen	7 Personelle Sicher-heit	BSI-Standard 100-2, Kapitel 3.4.2, B 1.0, B 1.13, B 1.2, B 1.3, B 1.8, M 2.1, M 2.192, M 2.193, M 2.199, M 2.225, M 2.226, M 2.30, M 2.312, M 2.336, M 2.337, M 2.35, M 2.39, M 2.5, M 2.550, M 3.1, M 3.2, M 3.26, M 3.33, M 3.5, M 3.50, M 3.6, M 3.96, M 6.59, M 6.61, M 6.65	A.7.1 Prior to employment A.7.2 During employment A.7.3 Termination and change of employment A.6.1 Internal organization	-	ORG 1.2, 1.3, 1.4, 1.5	4, 13, 14, 17	PR.AT-1,2,3,4,5	-
2	Umgang mit Dienstleistern, Lieferanten und Dritten	Beziehungen mit Dienstleistern, Lie-feranten und Drit-ten	6.2 Zusammenar-beit mit Externen 14.2 Evaluierung und Zertifizierung	B 1.11, B 1.17, M 2.250, M 2.251, M 2.253, M 2.254, M 2.356, M 2.4, M 2.475, M 2.516, M 2.517, M 2.539, M 2.541, M 2.554, M 3.55, M 5.33, M 5.87, M 5.88	A.15.1 Information secu-rity in supplier relation-ships	-	ORG 1.6	1, 2, 12	ID.BE-1,2	-

#	Kategorie	Sicherheitsmaß-nahme	Ö. Informations-sicherheitshandbuch Version 4.0.1	BSI IT-Grund-schutz[3]	ISO 27001:2013	ISA/IEC 62443 3-3	ISA/IEC 62443 2-1	CIS CSC Version 7.0	NIST CYBER SECURITY FRAME-WORK	ÖNORM A7700-4
		Leistungsvereinba-rungen mit Dienst-leistern und Liefe-ranten	15 Lieferanten-be-ziehungen	B 1.11, B 1.14, B 1.17, B 5.23, M 2.221, M 2.256, M 2.34	A.15.2 Supplier service de-livery management	-	ORG 1.6	1, 2, 12	ID.BE-3,4 PR.AT-3	-

2.2.2 Schutz

#	Kategorie	Sicherheitsmaß-nahme	Ö. Informations-sicherheitshandbuch Version 4.0.1	BSI IT-Grundschutz[4]	ISO 27001:2013	ISA/IEC 62443 3-3	ISA/IEC 62443 2-1	CIS CSC Version 7.0	NIST CYBER SECURITY FRAME-WORK	ÖNORM A 7700-4
3	Sicherheits-ar-chitektur	Systemkonfigu-ration	12.2.3 Dokumentation der Systemkonfigura-tion	B 1.10, B 1.9, B 4.2, B 5.25, M 2.1, M 2.201, M 2.219, M 2.62	A.12.1.1 Documented operating procedures A.12.5 Control of opera-tional software	SR 2.3, 2.4, 2.5, 2.7, 3.2, 3.3, 3.4, 3.5, 7.2, 7.6	ORG 2.3, CM 1.2, 1.3, NET 1.9, 1.10, 2.3, COMP 1.1, 2.2, 2.3, DATA 1.3, USER 1.14, 1.16, 1.18	1, 2, 5, 6, 7, 8, 9, 10, 11, 13, 15, 18,	PR.IP-1,3	4, 8

[4] Hinweis: Die BSI-Standards 200-1, 200-2 und 200-3 lösen seit Oktober 2017 die BSI-Standards der Reihe 100-x ab. Den IT-Grundschutz-Anwendern stellt das BSI zur erfolgreichen Migration eine „Anleitung zur Migration von Sicherheitskonzepten“ zur Verfügung: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/Migrationsleitfaden/Anleitung_zur_Migration.html

#	Kategorie	Sicherheitsmaß-nahme	Ö. Informations-sicherheitshandbuch Version 4.0.1	BSI IT-Grundschutz[4]	ISO 27001:2013	ISA/IEC 62443 3-3	ISA/IEC 62443 2-1	CIS CSC Version 7.0	NIST CYBER SECURITY FRAME-WORK	ÖNORM A 7700-4
		Vermögenswerte	8 Vermögenswerte und Klassifizierung von Informationen 8.1.1 Inventar der Vermögenswerte (Assets) mittels Strukturanalyse 14.1.10 Lizenzverwaltung und Versionskontrolle von Standardsoftware	B 1.0, B 1.1, BSI-Standard 100-2, Kapitel 4.2, BSI-Standard 100-2, Kapitel 4.3, M 1.33, M 1.34, M 2.139, M 2.195, M 2.217, M 2.218, M 2.225, M 2.226, M 2.235, M 2.309, M 3.6, M 5.88	A 8.1 Responsibility for assets A 8.2 Information classification	SR 7.8	CM 1.1, 1.2	1, 2, 9, 10, 11, 13, 15,	-	6.4, 7
		Netzwerk-segmentierung	13.1 Netzsicherheit	B 3.301, B 4.1, B 4.2, B 4.4, B 4.5, M 2.141, M 2.143, M 2.169, M 2.279, M 2.38, M 2.576, M 2.577, M 2.579, M 4.133, M 4.79, M 4.80, M 4.81, M 4.82, M 5.61, M 5.62, M 5.68, M 5.7, M 5.71, M 5.77, M 5.8, M 5.9	A.13.1 Network security management	SR 2.2, 5.1	NET 1.1, 1.2, 1.3, 2.2	1, 2, 5, 7, 8, 9, 11, 12, 13, 15	PR.AC-5	6.2, 6.5
		Netzwerksicherheit	13.1 Netzsicherheit	B 1.10, B 1.14, B 1.9, B 5.25, M 2.216, M 2.273, M 2.35, M 2.62, M 2.85	A.12.5 Control of operational software A.12.6 Technical vulnerability management	SR 1.13, 3.1, 5.2, 7.7	NET 1.4, 1.5, 1.6, 1.7, 1.8, 2.1	5, 7, 8, 9, 11, 13, 15	-	10.2

#	Kategorie	Sicherheitsmaß-nahme	Ö. Informations-sicherheitshandbuch Version 4.0.1	BSI IT-Grundschutz[4]	ISO 27001:2013	ISA/IEC 62443 3-3	ISA/IEC 62443 2-1	CIS CSC Version 7.0	NIST CYBER SECURITY FRAME-WORK	ÖNORM A 7700-4
		Kryptographie	10 Kryptographie	B 1.15, B 1.2, B 1.4, B 1.6, B 1.7, B 1.8, B 3.402, B 3.403, B 3.404, B 3.405, B 3.406, B 5.14, B 5.19, B 5.2, B 5.3, M 2.112, M 2.154, M 2.161, M 2.164, M 2.217, M 2.218, M 2.226, M 2.3, M 2.35, M 2.37, M 2.393, M 2.398, M 2.4, M 2.431, M 2.44, M 2.45, M 2.455, M 2.46, M 2.5, M 2.9, M 3.2, M 3.55, M 4.1, M 4.2, M 4.234, M 5.108, M 5.23, M 5.54, M 5.56, M 5.88, M 6.20, M 6.23, M 6.32, M 6.41	A.10.1 Cryptographic controls A 6.1.2 Segregation of duties A.8.3 Media handling A.11.2.7 Secure disposal or reuse of equipment A.11.2.9 Clear desk and clear screen policy A.12.2.1 Controls against malware A.12.3.1 Information backup A.13.2 Information transfer	SR 1.8, 1.9, *4.3*	DATA 1.7, 1.8, 1.9	5, 7, 8, 11, 13, 15, 18	-	10.1
4	System-admi-nistration	Administrative Zugangsrechte	9.1 Zugriffskontroll-politik 12.5 Protokollierung und Monitoring	M 2.220, M 2.20, M 2.38, M 4.312	A.9.2.3 Management of privileged access rights	SR 2.1	USER 2.2	4, 5, 8, 11, 13, 14, 18	PR.AT-2	9

#	Kategorie	Sicherheitsmaß-nahme	Ö. Informations-sicherheitshandbuch Version 4.0.1	BSI IT-Grundschutz[4]	ISO 27001:2013	ISA/IEC 62443 3-3	ISA/IEC 62443 2-1	CIS CSC Version 7.0	NIST CYBER SECURITY FRAME-WORK	ÖNORM A 7700-4
		Systeme und An-wendungen zur System-administ-ration	9.4 Fernzugriff 9.5 Zugriff auf Be-triebssysteme 9.6 Zugriff auf Anwendungen und In-formationen 12.5 Protokollierung und Monitoring	M 2.11, M 2.217, M 2.220, M 2.30, M 2.321, M 2.322, M 2.378, M 2.8, M 3.18, M 4.133, M 4.135, M 4.15, M 4.16, M 4.2, M 4.41, M 4.494, M 5.61, M 5.62, M 5.77	A.9.4 System and appli-cation access control	SR 5.4	-	4, 13, 14, 18	PR.AT-2	9
5	Identitäts- und Zugriffs-ma-nagement	Identifikation und Authentifi-kation	9 Zugriffskontrolle, Berechtigungssys-teme, Schlüssel- und Passwortverwaltung	B 1.18, B 4.4, B 4.5, B 5.15, M 2.169, M 2.214, M 2.220, M 2.30, M 2.457, M 2.5, M 2.7, M 2.71, M 2.8	A.9.1 Business require-ments of access control	SR 1.1, 1.2, 1.3, 1.4, 1.6, 1.7, 1.10, 1.11, 1.12	USER 1.1, 1.3, 1.6, 1.8, 1.9, 1.10, 1.11, 1.12., 1.15, 1.17	5, 4, 7, 11, 13, 14, 15, 18	PR.AC-1	9
		Autorisierung	9 Zugriffskontrolle, Berechtigungssys-teme, Schlüssel- und Passwortverwaltung	B 1.18, M 2.11, M 2.199, M 2.20, M 2.22, M 2.220, M 2.226, M 2.30, M 2.31, M 2.38, M 2.402, M 2.5, M 2.586, M 2.63, M 3.26, M 3.5, M 4.133, M 4.312, M 4.7, M 5.34	A.9.2 User access man-agement A 9.3 User responsibili-ties A 6.1.2 Segregation of duties	SR 1.5, 1.13, 2.1, 3.8, 4.1, 6.1, 7.7	NET 1.8, DATA 1.2, U-SER 1.2, 1.4, 1.5, 1.7, 2.1, 2.3, 2.4	1, 2, 4, 5, 7, 10, 11, 13, 14, 15, 18	ID.AM-5,6 PR.AC-1,4	6.3

#	Kategorie	Sicherheitsmaß-nahme	Ö. Informations-sicherheitshandbuch Version 4.0.1	BSI IT-Grundschutz[4]	ISO 27001:2013	ISA/IEC 62443 3-3	ISA/IEC 62443 2-1	CIS CSC Version 7.0	NIST CYBER SECURITY FRAME-WORK	ÖNORM A 7700-4
6	Systemwartung und Betrieb	Systemwartung und Betrieb	2.4 Informations-sicherheit im laufenden Betrieb 6.2 Zusammenarbeit mit Externen 12 Sicherheits-management im Betrieb 14.6 Wartung	B 1.10, B 1.11, B 1.14,B 1.7, B 1.9, B 5.21, B 5.24, B 5.25, B 5.27, B 5.4, M 2.162, M 2.164, M 2.172, M 2.216, M 2.217, M 2.220, M 2.251, M 2.252, M 2.253, M 2.254, M 2.256, M 2.34, M 2.4, M 2.487, M 2.546, M 2.568, M 2.62, M 2.66, M 2.80, M 2.85, M 2.9, M 4.176, M 4.494, M 4.65, M 4.78, M 4.93, M 4.94, M 5.150, M 5.87, M 5.88	A.14.1 Security require-ments of information systems A.14.2 Security in devel-opment and support processes A.11.2.4 Equipment maintenance	SR 4.2, 5.3	CM 1.3, 1.4, COMP 1.2, 2.1, 3.1, 3.2, 3.3, 3.4, 3.5, DATA 1.6, EVENT 1.9, AVAIL 2.2, 2.3	1, 2, 5, 6, 10, 11, 13	PR.IP-2 PR.MA-1,2	7
		Fernzugriff	9.4 Fernzugriff	B 2.10, B 3.203, B 3.404, B 3.405, B 5.8, M 1.33, M 2.218, M 2.309	A.6.2 Mobile devices and teleworking	SR 2.3, 2.6	NET 3.1, 3.2, 3.3	1, 4, 5, 11, 13	PR.AC-3	-

#	Kategorie	Sicherheitsmaß-nahme	Ö. Informations-sicherheitshandbuch Version 4.0.1	BSI IT-Grundschutz[4]	ISO 27001:2013	ISA/IEC 62443 3-3	ISA/IEC 62443 2-1	CIS CSC Version 7.0	NIST CYBER SECURITY FRAME-WORK	ÖNORM A 7700-4
7	Physische Sicherheit	Physische Sicherheit	11 Physische und um-gebungsbezogene Si-cherheit	B 2.3, B 1.15, B 2.1, B 2.10, B 2.12, B 2.2, B 2.3, B 3.203, B 3.406, B 5.8, M 1.1, M 1.12, M 1.13, M 1.16, M 1.17, M 1.18, M 1.19, M 1.2, M 1.22, M 1.28, M 1.29, M 1.33, M 1.45, M 1.46, M 1.49, M 1.53, M 1.55, M 1.56, M 1.58, M 1.6, M 1.61, M 1.75, M 1.78, M 1.79, M 1.80, M 2.112, M 2.16, M 2.17, M 2.18, M 2.218, M 2.309, M 2.37, M 2.4, M 2.431, M 2.6, M 2.90, M 3.26, M 4.1, M 4.2, M 4.234, M 4.29, M 5.4, M 5.5	A.11.1 Secure areas A.11.2 Equipment	-	ORG 3.1	1, 4, 5, 11, 13	PR.AC-2 PR.IP-5	9

2.2.3 Verteidigung

#	Kategorie	Sicherheitsmaß-nahme	Ö. Informations-sicherheitshand-buch Version 4.0.1	BSI IT-Grundschutz[5]	ISO 27001:2013	ISA/IEC 62443 3-3	ISA/IEC 62443 2-1	CIS CSC Version 7.0	NIST CYBER SECURITY FRAME-WORK	ÖNORM A 7700-4
8	Erkennung von Vorfällen	Erkennung	12.5 Protokollierung und Monitoring	B 1.6, B 1.8, B 5.22, M 2.110, M 2.133, M 2.154, M 2.220, M 2.273, M 2.35, M 2.500, M 2.568, M 2.64, M 2.9, M 4.135, M 4.227, M 4.25, M 4.34, M 4.430, M 4.5, M 4.81, M 4.93, M 5.150, M 5.9, M 6.23	A.12.4 Logging and monitoring A.12.2.1 Controls against malware A.12.6.1 Manage-ment of technical vulnerabilities A.14.2.8 System se-curity testing	SR 2.10, 2.12, 3.4	ORG 2.2, USER 1.13, EVENT 1.1	3, 6, 16, 19, 20	DE.AE-1, DE.CM-1,2,3,4,5,6, 7,8, DE.DP-1,2,3,4,5	12
		Protokollierung und Monitoring	12.5 Protokollierung und Monitoring	B 5.22, M 2.110, M 2.133, M 2.220, M 2.500, M 2.64, M 4.135, M 4.227, M 4.25, M 4.34, M 4.430, M 4.5, M 4.81, M 4.93, M 5.9	A.12.4 Logging and monitoring	SR 2.8, 2.9, 2.11, 3.9, 6.1	EVENT 1.2, 1.3, 1.4, 1.6	3, 6, 16, 19, 20	DE.CM-1	12
		Korrelation und Analyse	12.5 Protokollierung und Monitoring	B 5.22, M 2.110, M 2.133, M 2.220, M 2.500, M 2.64, M 4.135, M 4.227, M 4.25, M 4.34, M 4.430, M 4.5, M 4.81, M 4.93, M 5.9	A.12.4 Logging and monitoring	SR 6.2	EVENT 1.5, 1.7	3, 6, 16, 19, 20	DE.CM-1	-

[5] Hinweis: Die BSI-Standards 200-1, 200-2 und 200-3 lösen seit Oktober 2017 die BSI-Standards der Reihe 100-x ab. Den IT-Grundschutz-Anwendern stellt das BSI zur erfolgreichen Migration eine „Anleitung zur Migration von Sicherheitskonzepten“ zur Verfügung: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/Migrationsleitfaden/Anleitung_zur_Migration.html

#	Kategorie	Sicherheitsmaß-nahme	Ö. Informations-sicherheitshand-buch Version 4.0.1	BSI IT-Grundschutz[5]	ISO 27001:2013	ISA/IEC 62443 3-3	ISA/IEC 62443 2-1	CIS CSC Version 7.0	NIST CYBER SECURITY FRAME-WORK	ÖNORM A 7700-4
9	Bewältigung von Vorfällen	Vorfallsreaktion	16 Sicherheitsvor-fälle bzw. Informati-onssicherheitsereig-nisse (Incident Handling)	B 1.6, B 1.8, M 2.154, M 2.35, M 2.9, M 3.6, M 6.121, M 6.23, M 6.58, M 6.59, M 6.60, M 6.64, M 6.65	A.12.2.1 Controls against malware A.16.1.1 Responsi-bilities and proce-dures A.16.1.2 Reporting information security events A.16.1.3 Reporting information security weaknesses A.16.1.5 Response to information secu-rity incidents	-	ORG 2.2, EVENT 1.8	3, 6, 16, 17, 19, 20	PR.IP-9 RS.RP-1 RS.CO-1 RS.MI-1,2,3	-
		Vorfallsmeldung	16 Sicherheitsvor-fälle bzw. Informati-onssicherheitsereig-nisse (Incident Handling)	B 1.3, B 1.8, M 6.59, M 6.61, M 6.64, M 6.65	A.16.1.5 Response to information secu-rity incidents A.6.1.3 Contact with authorities	-	EVENT 1.8	3, 6, 16, 19, 20	RS.CO-1,2,3,4,5	-
		Vorfallsanalyse	16 Sicherheitsvor-fälle bzw. Informati-onssicherheitsereig-nisse (Incident Handling)	B 1.8, M 6.122, M 6.127, M 6.66, M 6.68	A.16.1.4 Manage-ment of information security incidents and improvements A.16.1.6 Learning from information se-curity incidents A.16.1.7 Collection of evidence	-	EVENT 1.8	3, 6, 16, 17, 19, 20	DE.AE-2,3,4,5 RS.AN-1,2,3,4	-

2.2.4 Resilienz

#	Kategorie	Sicherheitsmaß-nahme	Ö. Informations-sicherheitshand-buch Version 4.0.1	BSI IT-Grund-schutz[6]	ISO 27001:2013	ISA/IEC 62443 3-3	ISA/IEC 62443 2-1	CIS CSC Version 7.0	NIST CYBER SECURITY FRAME-WORK	ÖNORM A 7700-4
10	Betriebs-konti-nuität	Betriebskontinuitäts-management	17 Disaster Recovery und Business Conti-nuity	B 1.3, B 1.8, BSI-Standard 100-2, Kapitel 3, BSI-Standard 100-4	A.17.1 Informa-tion security conti-nuity	SR 3.6, 3.7, 7.1, 7.3, 7.4, 7.5	DATA 1.4, 1.5, AVAIL 1.1, 1.2, 1.3, 2.1, 2.4, 2.5	3, 10, 13	ID.BE-5 PR.DS-4 PR.IP-4	-
		Notfallmanagement	17 Disaster Recovery und Business Conti-nuity	B 2.4, B 2.9, M 1.52, M 6.103, M 6.104, M 6.157, M 6.18, M 6.53, M 6.75	A.17.2 Redundan-cies	-	AVAIL 1.1	10, 13,	PR.DS-4 PR.IP-10	-
11	Krisen-ma-nagement	Krisenmanagement	17 Disaster Recovery und Business Conti-nuity	B 1.3, B 1.8, BSI-Standard 100-2, Kapitel 3, BSI-Standard 100-4	A.17.1 Informa-tion security conti-nuity	-	AVAIL 1.1	10	PR.DS-4 PR.IP-10	-

[6] Hinweis: Die BSI-Standards 200-1, 200-2 und 200-3 lösen seit Oktober 2017 die BSI-Standards der Reihe 100-x ab. Den IT-Grundschutz-Anwendern stellt das BSI zur erfolgreichen Migration eine „Anleitung zur Migration von Sicherheitskonzepten“ zur Verfügung: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/Migrationsleitfaden/Anleitung_zur_Migration.html

3 Versionshistorie

Bei diesem Dokument handelt es sich um die Version 3.0 vom 23.03.2020.

Änderungen, Anpassungen sowie Detaillierungen in der Version 2.0 vom 29.10.2018 gegenüber der Version 1.0 vom 21.08.2018 betreffen vor allem das Mapping auf den **BSI IT-Grundschutz** und auf den Teil **3-3** der Normenreihe **IEC 62443**. Die Versionen 1.0 und 2.0 werden auf Anfrage an nis@bka.gv.at zur Verfügung gestellt.

Änderungen und Anpassungen der Version 3.0 gegenüber der Version 2.0 resultieren aus dem Abgleich mit der nach der Veröffentlichung der Version 2.0 in Kraft getretenen NISV und betreffen einerseits die Kapitel „Einleitung“ und „NIS-Kooperationsgruppe“ sowie das Mapping auf folgende Standards/Normen:

- **IEC 62443 Teil 3-3** („System security requirements and security levels”, edition 1.0, 2013-08)
- **IEC 62443 Teil 2-1** (“Security program requirements for IACS asset owners”, draft - CDV, 2019-08)
- **ÖNORM A 7700-4** (Ausgabe vom 2019-10-01)
- **CEC CIS Version 6.0** (wurde entfernt).

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundeskanzleramt, Ballhausplatz 2, 1010 Wien
Autoren: Bundeskanzleramt Abteilung I/8 (Cyber Security, GovCERT, NIS-Büro und ZAS) und BMI/II/BVT/5.3-NIS
Wien, 2020
Stand: 23. März 2020

Abschließende Anmerkungen:
Es wird darauf hingewiesen, dass Änderungen vorbehalten sind.
Alle in diesem NIS Fact Sheet verwendeten personenbezogenen Bezeichnungen gelten gleichermaßen für alle Geschlechter.

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