Zertifizierungsprogramm P92

Zertifizierter NIS2-Officer
gem. EU-Richtlinie 2022/2555

Version 1.0: 2024-09-30

Medieninhaber und Hersteller
Austrian Standards plus GmbH Heinestraße 38, 1020 Wien

E-Mail: certification@austrian-standards.at
Internet: www.austrian-standards.at

Inhaltsverzeichnis

1 Geltungsbereich 3

2 Anforderungen an die Kompetenz 3

2.1 Kompetenz- & Tätigkeitsprofil 3

2.2 Anforderungen an Wissen und Fertigkeiten 3

2.2.1 Technische Kenntnisse im Bereich Sicherheit von Netz- und Informationssystemen 3

2.2.2 Anwendbarkeit und Umsetzung von Netz- und Informationssystemsicherheit 4

2.2.3 Regulatorisches Wissen in Bezug auf Netz- und Informationssicherheit 4

3 Prüfung 4

4 Bewertungskriterien 5

5 Zertifizierungsvoraussetzungen Erst-Zertifizierung 5

6 Beschwerde, Einspruch, Prüfungseinsicht/-auskunft 5

7 Rezertifizierung 5

7.1 Kriterien zur Verlängerung des Zertifikates 5

7.2 Ausstellung des Zertifikates 6

7.3 Fristen 6

1 Geltungsbereich

Das vorliegende Zertifizierungsprogramm legt die Vorgangsweise zur Zertifizierung der Kompetenz von Personen als NIS2-Officer gem. der EU-Richtlinie 2022/2555[1] durch Austrian Standards plus Certification (AS+C), dem Geschäftsbereich Zertifizierung der Austrian Standards plus GmbH, fest.

Gegenstand der Zertifizierung ist ausschließlich die Kompetenz natürlicher Personen.

Die Zertifizierung erfolgt nach den Grundsätzen der ISO/IEC 17024[2].

2 Anforderungen an die Kompetenz

2.1 Kompetenz- & Tätigkeitsprofil

Zertifizierte Personen verfügen über technisches, rechtliches und organisatorisches Wissen in Bezug auf nationale und europäische Regelungen im Bereich der Netz- und Informationssicherheit. Sie sind kompetent, Prozesse und Maßnahmen in Bezug auf Netz- und Informationssicherheit auf Grundlage der Europäischen Richtlinie 2022/ 2055, zu definieren, zu steuern und zu überwachen. Sie kennen die Anforderungen an Berichtspflichten und durchzuführenden Maßnahme im Sinne des Art 23 der EU-Richtlinie 2022/2055. Sie können Risikomanagementmaßnahmen auf deren Notwendigkeit im Sinne des Art 21 der EU-Richtlinie 2022/2555 hin definieren und deren Umsetzung überwachen.

2.2 Anforderungen an Wissen und Fertigkeiten

Personen, die gemäß diesem Zertifizierungsschema zertifiziert sind, müssen Wissen und Fertigkeiten gemäß der Abschnitte 2.2.1 bis 2.2.3 aufweisen.

2.2.1 Technische Kenntnisse im Bereich Sicherheit von Netz- und Informationssystemen

Zertifizierte Personen

- kennen die Cybersecurity-Prinzipien sowie die damit zusammenhängenden Normen/Standards.
- verstehen, wie Systeme zur Bedrohungserkennung und -verhinderung eingesetzt werden können.
- verfügen über Kenntnisse in Bezug auf Software-Sicherheit sowie Sicherheitswerkzeugen.

[1] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (Text von Bedeutung für den EWR).

[2] ISO/IEC 17024:2012-07 Konformitätsbewertung - Allgemeine Anforderungen an Stellen, die Personen zertifizieren.

2.2.2 Anwendbarkeit und Umsetzung von Netz- und Informationssystemsicherheit

Zertifizierte Personen

- verfügen über umfassendes Wissen im Zusammenhang mit dem behördlichen NIS-2-Prozess und sind kompetent das NIS2-Self-Assessment, die Registrierung und Selbstdeklaration vorzubereiten und zu begleiten.
- kennen die Anforderungen an ein Risikomanagement- sowie Managementsystem von Netz- und Informationssystemen im Sinne der EU-Richtlinie 2022/2555.
- können IT-relevante Sicherheitsvorfälle erkennen und geeignete Maßnahmen zur Bewältigung definieren.
- können Risikomanagementmaßnahmen definieren, bewerten und überwachen.
- können datenschutzrechtliche Implikationen bei der Maßnahmenwahl und bei der Meldung von Cybersicherheitsvorfällen feststellen.
- sind kompetent, bei festgestellten Mängeln, geeignete Maßnahmen zu definieren sowie einen Maßnahmenplan zu erstellen.

2.2.3 Regulatorisches Wissen in Bezug auf Netz- und Informationssicherheit

Zertifizierte Personen

- kennen die Richtlinie 2022/2555 und die im Zusammenhang stehende delegierten Rechtsakte der europäischen Union und das innerstaatliche Umsetzungsgesetz.
- kennen die nationalen zuständigen Institutionen in Bezug auf Netz- und Informationssicherheit.
- verfügen über Kenntnisse hinsichtlich Aufgaben, Zuständigkeiten sowie Strukturen der Cybersicherheitsbehörde.
- können beurteilen, ob ein Unternehmen in den NIS2-Anwendungsbereich fällt.

3 Prüfung

Die Prüfung wird in Form eines Single-Choice-Tests abgehalten und umfasst 45 Fragen aus den 3 Themengebieten gemäß Abschnitt 2.2.1 bis 2.2.3. wie folgt:

- 15 Fragen gem. Abschnitt 2.2.1
- 15 Fragen gem. Abschnitt 2.2.2
- 15 Fragen gem. Abschnitt 2.2.3

Von den jeweils 15 Fragen gem. Abschnitt 2.2.1 bis 2.2.3 entfällt ein Teil auf Wissensfragen und ein der andere Teil auf Fallbeispiele (Case Studies). Bei den Fallbeispielen (Case Studies) muss der Kandidat theoretisches Wissen auf reale Situationen anwenden.

Die maximale Dauer der schriftlichen Prüfung ist mit 60 Minuten festgelegt.

Die Nutzung von Fachliteratur, Vortragsunterlagen, Mitschriften sowie die Nutzung des Internets (zu Recherchezwecken) ist in den Grenzen des vorgegebenen Zeitrahmens erlaubt.

4 Bewertungskriterien

Es können maximal 45 Punkte erreicht werden, wobei jede richtig beantwortete Frage mit einem Punkt bewertet wird.

Zur positiven Absolvierung der Gesamtprüfung müssen mindestens 60% der Gesamtpunktzahl (=27 von insgesamt 45 Punkten) erreicht werden.

5 Zertifizierungsvoraussetzungen Erst-Zertifizierung

Folgende Voraussetzung muss für die Ausstellung eines Zertifikates erfüllt sein:

1. Nachweis einer zweijährigen Berufserfahrung im Bereich Netz- und Informationssicherheit (rechtlich, organisatorisch oder technisch) oder einer facheinschlägigen Ausbildung (z.B. HTL) oder eines Studiums.
2. Nachweis einer Ausbildung im Ausmaß von mind. 24 Stunden auf den Inhalten gem. 2.2.1 bis 2.2.3 oder der Nachweis von äquivalenten Ausbildungen
3. positives Prüfungsergebnis (gem. Abschnitt 4 Bewertungskriterien)

Die Zertifikate haben eine Gültigkeit von 3 Jahren.

6 Beschwerde, Einspruch, Prüfungseinsicht/-auskunft

6.1 Einspruch: Prüfungsteilnehmende haben das Recht, Einspruch gegen das Prüfungsergebnis einzulegen. Die Zertifizierungsstelle von Austrian Standards folgt der in der ISO/IEC 17024 vorgegebenen Definition eines Einspruchs: „Mit dem Einspruch bringt der Anbieter eines Gegenstandes der Konformitätsbewertung gegenüber der Konformitätsbewertungsstelle sein Verlangen zum Ausdruck, die Entscheidung bezüglich dieses Gegenstandes zu überprüfen“.

6.2 Beschwerde: Prüfungsteilnehmende haben das Recht, Beschwerde bei der Zertifizierungsstelle einzulegen. Die Zertifizierungsstelle von Austrian Standards folgt der in der ISO/IEC 17024 vorgegebenen Definition einer Beschwerde: „Mit der Beschwerde bringt eine Person oder eine Organisation ihre Unzufriedenheit bezüglich der Tätigkeit der Konformitätsbewertungsstelle zum Ausdruck und erwartet eine Antwort“.

Beschwerden und Einsprüche sind schriftlich bei der Zertifizierungsstelle einzureichen.

6.3 Prüfungseinsicht und -auskunft: Eine Prüfungseinsicht sowie eine Prüfungsauskunft (erreichte Punkteanzahl) kann ausschließlich bei Nicht-Bestehen der Prüfung und im Rahmen eines Einspruchsverfahrens vorgenommen/erteilt werden.

7 Rezertifizierung

7.1 Kriterien zur Verlängerung des Zertifikates

Zur Verlängerung des Zertifikates muss die Zertifikatsinhaberin/der Zertifikatsinhaber die folgenden Kriterien erfüllen:

7.1.1 Die Zertifikatsinhaberin/der Zertifikatsinhaber muss Nachweise über facheinschlägige Weiterbildungen im Ausmaß von mindestens 24 Stunden für den gesamten Zertifizierungszyklus erbringen.

7.1.2 Die Zertifikatsinhaberin/der Zertifikatsinhaber muss Nachweise über die aufrechte, einschlägige Tätigkeit erbringen. Dies hat in Form von Tätigkeits- bzw. Projektbeschreibung zu erfolgen.

7.2 Ausstellung des Zertifikates

Nach Erfüllung aller Kriterien gemäß 7.1.1 und 7.1.2 wird das Zertifikat für drei Jahre verlängert.

7.3 Fristen

Die Rezertifizierung muss vor dem Ablauf des Zertifikates erfolgen. In Ausnahmefällen kann die Rezertifizierung auch nach Ablauf des Zertifikates erfolgen. Hierbei gelten folgende Bedingungen:

7.3.1 Erfolgt die Rezertifizierung nach Ablauf der Gültigkeit eines Zertifikats innerhalb eines Zeitraums von maximal sechs Monaten, wird die Rezertifizierung gemäß den Kriterien und dem Prozess gemäß Abschnitt 7.1 durchgeführt. Andernfalls ist eine Prüfung im Umfang der Erstzertifizierung gemäß Abschnitt 3 durchzuführen.

7.3.2 Die Gültigkeit des Zertifikats richtet sich immer nach dem Datum der Erstzertifizierung. Das heißt, es wird immer vom Datum der Erstzertifizierung ausgegangen, unabhängig von dem Datum der tatsächlich erfolgten Rezertifizierung.