NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Číslo: 06431/2024/SRD/OKD-001

Bratislava 30.04.2024

Metodika posudzovania spôsobilosti manažéra kybernetickej bezpečnosti

Štandard pre posudzovanie spôsobilosti na výkon roly manažéra kybernetickej bezpečnosti v zmysle požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Verzia	1.0
Dátum vydania	10. máj 2024
Dátum účinnosti	13. máj 2024

Národný bezpečnostný úrad | Budatínska 30 | 851 06 Bratislava | Slovenská republika
tel.: +421 2 6869 1111 | podatelna@nbu.gov.sk | www.nbu.gov.sk

Obsah

1 Kvalifikácia manažéra kybernetickej bezpečnosti

1.1 Kvalifikačné požiadavky na výkon roly manažéra kybernetickej bezpečnosti

Kvalifikácia je súhrn odborných vedomostí, zručností a kompetencií, ktoré sú potrebné na vykonávanie pracovných činností manažéra kybernetickej bezpečnosti.

Požiadavky na kvalifikáciu manažéra kybernetickej bezpečnosti sú stanovené znalostným štandardom, ktorý je pre rolu manažéra kybernetickej bezpečnosti uvedený v prílohe č. 5 vyhlášky č. 492/2022 Z. z. ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti (ďalej len „vyhláška č. 492/2022 Z. z.“).

Všeobecná charakteristika vzdelávacích potrieb pre jednotlivé kategórie používateľov informačno-komunikačných technológií je uvedená v prílohe č. 1 vyhlášky č. 492/2022 Z. z.

Úrovne vzdelávacích cieľov sú uvedené v prílohe č. 2 vyhlášky č. 492/2022 Z. z.

1.2 Minimálne požiadavky na vzdelanie a prax

Minimálne kvalifikačné požiadavky na úroveň vzdelania a prax osoby, ktorá má vykonávať úlohy manažéra kybernetickej bezpečnosti sú stanovené vo vyhláške č. 492/2022 Z. z. ako aj v certifikačnej schéme overovania odbornej spôsobilosti manažéra kybernetickej bezpečnosti zverejnenej na webovom sídle Národného bezpečnostného úradu.

Minimálne odporúčané požiadavky na kvalifikáciu a prax sú nasledujúce:

Vzdelanie a požadovaný doklad	**Prax a spôsob jej preukázania (alternatívy predložených dokumentov)**
Úplné stredné všeobecné vzdelanie a úplné stredné odborné vzdelanie (doklad o získanom stupni vzdelania a o získanej kvalifikácii)	• najmenej **7 rokov praxe** v oblasti informačných technológií (životopis s uvedením kontaktu na overiteľnú referenciu) • z toho najmenej **5 rokov praxe** v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT • medzinárodne uznaný certifikát sa považuje za započítateľnú odbornú prax 1 rok
Vysokoškolské vzdelanie prvého stupňa (doklady o absolvovaní štúdia)	• najmenej **5 rokov praxe** v oblasti informačných technológií (životopis s uvedením kontaktu na overiteľnú referenciu) • z toho najmenej **3 roky praxe** v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT • medzinárodne uznaný certifikát sa považuje za započítateľnú odbornú prax 1 rok
Vysokoškolské vzdelanie druhého a tretieho stupňa (doklady o absolvovaní štúdia)	• najmenej **3 roky praxe** v oblasti informačných technológií (životopis s uvedením kontaktu na overiteľnú referenciu) • z toho najmenej **1 rok praxe** v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT

Vzdelanie a požadovaný doklad	Prax a spôsob jej preukázania (alternatívy predložených dokumentov)
	• medzinárodne uznaný certifikát sa považuje za započítateľnú odbornú prax 1 rok

Tieto požiadavky môžu orientačne slúžiť aj pri obsadzovaní pozície manažéra kybernetickej bezpečnosti necertifikovanou osobou na základe vlastného posúdenia prevádzkovateľa základnej služby, na základe predloženia medzinárodného certifikátu vydaného v neakreditovanom režime.

2 Posudzovanie spôsobilosti

2.1 Metódy posudzovania spôsobilostí

Za určenie manažéra kybernetickej bezpečnosti je podľa § 19 ods. 1 v spojení s § 20 ods. 4 písm. a) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“) zodpovedný prevádzkovateľ základnej služby. Preto aj rozhodnutie o tom, či manažér kybernetickej bezpečnosti spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti je právom a povinnosťou štatutárneho orgánu prevádzkovateľa základnej služby, alebo osoby, ktorá je štatutárnym orgánom poverená na vydanie rozhodnutia.

Manažér kybernetickej bezpečnosti **musí byť spôsobilý na výkon tejto roly**. Overenie spôsobilosti sa dá vykonávať priamym overovaním kvalifikácie, alebo prostredníctvom požiadavky na predloženie osvedčenia o vzdelaní a kvalifikácii, alebo prostredníctvom požiadavky na príslušnú certifikáciu, ktorá zahŕňa overenie vedomostí, zručností, kompetencií, odbornej praxe, oblasti vzdelania a stupňa vzdelania.

Spôsobilosť na výkon roly, t. j. či uchádzač o zamestnanie, alebo potenciálny dodávateľ spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti, je pre potreby určenia manažéra kybernetickej bezpečnosti možné objektívne overiť prostredníctvom nasledujúcich metód:

- Posúdenie na základe predloženia **osvedčenia o absolvovaní akreditovaného vzdelávacieho programu** podľa osobitného predpisu.[1)]
- Posúdenie na základe predloženia **certifikátu vydaného v zmysle platnej certifikačnej schémy**.

Doplňujúcou informáciou pre prevádzkovateľa základnej služby o spôsobilostiach uchádzača alebo potenciálneho dodávateľa môže byť aj posúdenie na základe predloženia medzinárodného certifikátu vydaného v neakreditovanom režime.

V zmysle § 29 zákona č. 69/2018 Z. z. je prevádzkovateľ základnej služby povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom č. 69/2018 Z. z. vykonaním auditu kybernetickej bezpečnosti v rozsahu stanovenom podľa všeobecne záväzného právneho predpisu. Audit kybernetickej bezpečnosti vykonáva certifikovaný audítor kybernetickej bezpečnosti.

Audítor je oprávnený v rámci preverovania účinnosti prijatých bezpečnostných opatrení posúdiť aj požiadavku § 20 ods. 4 písm. a) zákona č. 69/2018 Z. z. vrátane toho, či manažér kybernetickej bezpečnosti spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti.

2.2 Osvedčenie o absolvovaní akreditovaného vzdelávacieho programu

Vhodnou formou posúdenia spôsobilostí je požiadať uchádzača, aby predložil **osvedčenie o absolvovaní ďalšieho odborného vzdelávanie v akreditovanom vzdelávacom programe** pre manažérov kybernetickej bezpečnosti.

Pozn.: *Osvedčenie o absolvovaní odborného vzdelávacieho programu pre manažéra kybernetickej bezpečnosti sú oprávnené vydávať len vzdelávacie inštitúcie, ktoré boli na tento účel akreditované podľa osobitného predpisu[1)] Ministerstvom školstva, výskumu, vývoja a mládeže Slovenskej republiky.*

[1)] § 9 ods. 2 zákona č. 568/2009 Z. z. o celoživotnom vzdelávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

2.3 Certifikáty vydané podľa certifikačnej schémy

Manažéri kybernetickej bezpečnosti **môžu byť certifikovaní v zmysle zákona č. 69/2018 Z. z. podľa certifikačnej schémy overovania odbornej spôsobilosti manažéra kybernetickej bezpečnosti**. Vlastníkom certifikačnej schémy je Národný bezpečnostný úrad.

Služby posudzovania zhody vykonávajú akreditované orgány posudzovania zhody podľa certifikačnej schémy a podľa odporúčaní medzinárodne akceptovaných štandardov alebo iných vecne obdobných postupov príslušným na certifikáciu osôb.

Orgán posudzovania zhody je oprávnený vydávať certifikát manažéra kybernetickej bezpečnosti len za predpokladu, že je na to akreditovaný vnútroštátnym akreditačným orgánom, t. j. Slovenskou národnou akreditačnou službou (SNAS) pre oblasť certifikácie manažérov v súlade s certifikačnou schémou. Postavenie SNAS a jej pôsobnosť určuje zákon č. 23/2023 Z. z. o akreditácii orgánov posudzovania zhody.

Certifikačná schéma je záväzná pre všetky akreditované orgány posudzovania zhody, a to v súlade s STN EN ISO/IEC 17024: 2013 Posudzovanie zhody. Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb.

Za certifikačný proces sú zodpovedné akreditované orgány posudzovania zhody. V certifikačnom procese certifikačný orgán určí, či manažér kybernetickej bezpečnosti spĺňa certifikačné požiadavky. Uvedené zahŕňa podanie žiadosti, posúdenie, certifikačnú skúšku, rozhodnutie o certifikácii, recertifikácii a používaní certifikátov, loga a certifikačných značiek.

Úrad zverejňuje na svojom webovom sídle:

- okruhy a príklady otázok na vykonanie odbornej skúšky a usmernenie na ich používanie,
- vzor žiadosti o vykonanie odbornej skúšky a
- vzor certifikátu manažéra kybernetickej bezpečnosti.

2.4 Certifikáty vydané v neakreditovanom režime

Za certifikáty vydané v neakreditovanom režime, relevantné pre oblasť kybernetickej a informačnej bezpečnosti, najmä v kontexte výkonu činností súvisiacich s výkonom role manažéra kybernetickej bezpečnosti sa považujú najmä medzinárodne uznané odborné certifikáty uvedené v prílohe č. 1 tohto metodického usmernenia.

Predložením medzinárodného odborného certifikátu uchádzač o zamestnanie alebo potenciálny dodávateľ deklaruje, že je odborne spôsobilý vykonávať činnosti súvisiace s výkonom role manažéra kybernetickej bezpečnosti.

Zoznam certifikátov uvedených v prílohe č. 1 má informatívny charakter a nie je konečným zoznamom uznávaných certifikátov. Certifikáty, ktoré nie sú uvedené v prílohe č. 1 sa posudzujú ad hoc podľa kontextu výkonu činností role manažéra kybernetickej bezpečnosti.

Príloha č. 1 Informatívny zoznam odborných certifikátov

Skratka	Názov	Vydavateľ
CISA	Certified Information Systems Auditor	ISACA
CISM	Certified Information Security Manager	
CRISC	Certified In Risk and Information Systems Control	
CDPSE	Certified Data Privacy Security Engineer	
CISSP	Certified Information Systems Security Professional	(ISC)²
CSSLP	Certified Secure Software Lifecycle Professional	
CCSP	Certified Cloud Security Professional	
SSCP	Systems Security Certified Practitioner	
CCFP	Certified Cyber Forensics Professional	
CASP	CompTIA Advanced Security Practitioner	CompTIA
CSA+	CompTIA Cyber Security Analyst	
Security+	CompTIA Security+	
Pentest+	CompTIA Pentest+	
OSCP	Offensive Security Certified Professional	Offensive Security
OSWP	Offensive Security Wireless Professional	
OSCE	Offensive Security Certified Expert	
OSEE	Offensive Security Exploitation Expert	
OSWE	Offensive Security Web Expert	
GISF	GIAC Information Security Fundamentals	GIAC
GSEC	GIAC Security Essentials Certification	
GISP	GIAC Information Security Professional	
GPPA	GIAC Certified Perimeter Protection Analyst	
GCIA	GIAC Certified Intrusion Analyst	
GCED	GIAC Certified Enterprise Defender	
GPEN	GIAC Certified Penetration Tester	
GWAPT	GIAC Certified Web Application Penetration Tester	
GSTRT	GIAC Strategic Planning, Policy, and Leadership	
GSNA	GIAC Systems and Network Auditor	
GCFA	GIAC Certified Forensic Analyst	
GLEG	GIAC Law of Data Security & Investigations	
GSE	GIAC Security Expert	
CEH	Certified Ethical Hacker	EC-Council
CHFI	Certified Hacking Forensic Investigator	
ECIH	EC-Council Certified Incident Handler	
ENSA	EC-Council Network Security Administrator	
CCISO	Certified Chief Information Security Officer	

EDRP	EC-Council Disaster Recovery Professional	
LA27k	ISO/IEC 27001 Lead Auditor	ISO