NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Certifikačná schéma overovania odbornej spôsobilosti manažéra kybernetickej bezpečnosti

Verzia 1.2 zo dňa 12.01.2024 účinná od 1.2.2024

1 TERMÍNY A DEFINÍCIE ... 3

2 ÚVOD ... 5

2.1 ROZSAH CERTIFIKÁCIE ... 5
2.2 PRÁVNY ZÁKLAD A NORMATÍVNE KRITÉRIÁ ... 5
2.3 CERTIFIKAČNÉ ROLY ... 5
2.3.1 Vlastník certifikačnej schémy ... 5
2.3.2 Orgány posudzovania zhody ... 5
2.3.3 Akreditačný orgán ... 6

3 KRITÉRIÁ CERTIFIKÁCIE ... 7

3.1 VŠEOBECNÉ POŽIADAVKY NA SPÔSOBILOSŤ ... 7
3.1.1 Minimálne všeobecné požiadavky na spôsobilosť ... 7
3.1.2 Minimálne požiadavky na vzdelanie a prax ... 7
3.1.3 Všeobecné predpoklady na výkon činnosti manažéra ... 7
3.1.4 Špecifické kľúčové kompetencie ... 8
3.2 OSOBITNÉ POŽIADAVKY NA SPÔSOBILOSŤ ... 8

4 POSÚDENIE ZHODY ... 12

4.1 POČIATOČNÉ KRITÉRIÁ CERTIFIKÁCIE ... 12
4.2 POSUDZOVANIE KANDIDÁTOV ... 12
4.3 ODBORNÁ SKÚŠKA ... 12
4.3.1 Obsah odbornej skúšky ... 12
4.3.2 Požiadavky na skúšobné otázky ... 13
4.3.3 Príprava otázok na odbornú skúšku ... 13
4.3.4 Kvalifikačné požiadavky na skúšajúcich ... 14
4.3.5 Termín a miesto vykonania odbornej skúšky ... 14
4.3.6 Priebeh odbornej skúšky ... 14
4.3.7 Vyhodnotenie odbornej skúšky ... 14

5 CERTIFIKÁT ... 16

5.1 UDELENIE CERTIFIKÁTU ... 16
5.2 DOHĽAD NAD ČINNOSŤOU CERTIFIKOVANÉHO MANAŽÉRA ... 16
5.3 OBNOVA CERTIFIKÁTU A PREDĹŽENIE PLATNOSTI CERTIFIKÁTU ... 17
5.3.1 Obnova platnosti certifikátu manažéra ... 17
5.3.2 Predĺženie platnosti certifikátu manažéra ... 17
5.3.3 Zmena predmetu certifikácie ... 18
5.4 POZASTAVENIE ALEBO ZRUŠENIE CERTIFIKÁTU MANAŽÉRA ... 18
5.4.1 Pozastavenie alebo zrušenie platnosti certifikátu orgánom posudzovania zhody ... 18
5.4.2 Pozastavenie platnosti certifikátu na základe podnetu NBÚ ... 18
5.4.3 Pozastavenie platnosti certifikátu na základe požiadavky manažéra kybernetickej bezpečnosti ... 18
5.4.4 Ukončenie platnosti certifikátu ... 19

6 VYBAVOVANIE SŤAŽNOSTÍ ... 19

7 VEDENIE EVIDENCIÍ ... 19

8 PRÍSTUP K CERTIFIKAČNEJ SCHÉME 19

ETICKÝ KÓDEX MANAŽÉRA KYBERNETICKEJ BEZPEČNOSTI 20

1 TERMÍNY A DEFINÍCIE

Termín	Význam
akreditácia	osvedčenie treťou stranou týkajúce sa ogánu posudzovania zhody, kotrým sa formálne potvrdzuje jeho kompetentnosť, nestrannnosť a konzistentné fungovanie v rámci konkrétnych činností posudzovania zhody (STN EN ISO/IEC 17000: 2022)
osvedčovanie	vydanie vyhlásenia na základe rozhodnutia, o tom, že bolo preukázané splnenie určených požiadaviek (STN EN ISO/IEC 17000: 2022)
Audit	systematický, nezávislý a zdokumentovaný proces získavania záznamov, konštatovaní faktov alebo iných dôležitých informácií a ich objektívneho posudzovania s cieľom určiť rozsah, v akom sa splnili určené požiadavky (ISO/IEC 17024:2012)
autorizácia	vládne splnomocnenie orgánu posudzovania zhody vykonávať určené činnosti posudzovania zhody (STN EN ISO/IEC 17000: 2022)
certifikačné požiadavky	súbor stanovených požiadaviek, vrátane požiadaviek schémy, ktoré je potrebné splniť, na preukázanie alebo udržanie certifikácie (ISO/IEC 17024:2012)
certifikačný orgán	orgán vykonávajúci posudzovanie zhody treťou stranou podľa certifikačnej schémy (ISO/IEC 17024:2012)
certifikačný proces	činnosti, na základe ktorých certifikačný orgán určí, že osoba spĺňa certifikačné požiadavky , zahŕňa podanie žiadosti, posúdenie, rozhodnutie o certifikácii, recertifikácii a používanie certifikátov, loga a certifikačných značiek (ISO/IEC 17024:2012)
certifikát	dokument vydaný certifikačným orgánom v súlade s ustanoveniami tejto medzinárodnej normy, osvedčujúci, že menovaná osoba splnila certifikačné požiadavky (ISO/IEC 17024:2012)
Dohľad	systematické opakovanie činností posudzovania zhody ako základ udržania platnosti potvrdenia o zhode (STN EN ISO/IEC 17000: 2022)
Dozor	osoba poverená certifikačným orgánom, ktorá pomáha dohliadať alebo dohliada na skúšku, ale nehodnotí kompetentnosť kandidáta
kandidát	žiadateľ, ktorý splnil stanovené predpoklady a bol zaradený do certifikačného procesu (ISO/IEC 17024:2012)
kvalifikácia	preukázané vzdelanie, odborná príprava a pracovné skúsenosti
objekt posudzovania zhody	akýkoľvek konkrétny materiál, produkt, inštalácia, proces, systém, osoba alebo orgán, ktorých sa týka posudzovanie zhody (ISO/IEC 17065: 2013, ISO/IEC 17021-1:2015, ISO/IEC 17024:2012)
odvolanie sa	žiadosť žiadateľa, kandidáta alebo certifikovanej osoby o opätovné zváženie akéhokoľvek rozhodnutia certifikačného orgánu, ktoré sa týka ním požadovaného stavu certifikácie (ISO/IEC 17024:2012)
orgán posudzovania zhody	orgán, ktorý vykonáva služby posudzovania zhody (ISO/IEC 17024:2012)
posudzovanie	proces, ktorým sa hodnotí ako konkrétna osoba splnila požiadavky certifikačnej schémy (ISO/IEC 17024:2012)
posudzovanie zhody	preukázanie splnenia určených požiadaviek (STN EN ISO/IEC 17000: 2022)
skúšajúci	kompetentná osoba na vykonávanie a klasifikovanie skúšky, ak skúška vyžaduje odborné hodnotenie

Termín	Význam
skúšanie (testovanie)	určenie jednej alebo viacerých vlastností predmetu posudzovania zhody podľa postupu. Termín skúšanie sa zvyčajne týka materiálov, produktov alebo procesov. V niektorých aplikačných oblastiach sa uprednostňuje z angličtiny prevzatý termín testovanie, resp. test (napr. testovanie hypotéz, testovanie softvéru a pod.). (ISO/IEC 17000: 2022)
Skúška	mechanizmus tvoriaci časť posudzovania, ktorým sa hodnotí kompetentnosť kandidáta jedným alebo viacerými spôsobmi, ako písomne, ústne, prakticky alebo pozorovaním, podľa nadefinovania v certifikačnej schéme
spôsobilosť	schopnosť uplatniť vedomosti a zručnosti na dosiahnutie zamýšľaných výsledkov
sťažnosť	vyjadrenie nespokojnosti, inej ako v odvolaní, predložené certifikačnému orgánu jednotlivcom alebo organizáciou, vo veci činností tohto orgánu alebo certifikovanej osoby, s očakávaním odpovede (ISO/IEC 17024:2012)
špecifikácia spôsobilostí	normatívny dokument definujúci kritériá spôsobilosti
vlastník schémy	organizácia zodpovedná za rozvoj a udržiavanie certifikačnej schémy (ISO/IEC 17024:2012)
Žiadateľ	osoba, ktorá podala žiadosť o prijatie do certifikačného procesu (ISO/IEC 17024:2012)

2 ÚVOD

2.1 ROZSAH CERTIFIKÁCIE

Predmet certifikácie	Manažér kybernetickej bezpečnosti podľa osobitných predpisov[1)]
Opis práce a úloh	Plánovanie, riadenie implementácie, prevádzka a udržiavanie bezpečnostných opatrení a riadenie súladu s požiadavkami ustanovenými právnymi predpismi upravujúcimi oblasť kybernetickej bezpečnosti a informačné technológie vo verejnej správe

2.2 PRÁVNY ZÁKLAD A NORMATÍVNE KRITÉRIÁ

Táto certifikačná schéma sa opiera najmä o nasledujúcu právnu úpravu a technické normy:

- Zákon 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.“);
- Vyhláška Národného bezpečnostného úradu č. 492/2022 Z. z., ktorou sa ustanovujú znalostné štandardy v kybernetickej bezpečnosti (ďalej len „vyhláška č. 492/2022 Z. z.“);
- Vyhláška Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti;
- Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška č. 362/2018 Z. z.“);
- Zákon č. 56/2018 Z.z. o posudzovaní zhody výrobku, sprístupňovaní určeného výrobku na trhu a o zmene a doplnení niektorých zákonov v znení zákona č. 259/2021 Z. z. (ďalej len „zákon č. 56/2018“);
- ISO/IEC 17024:2012 Posudzovanie zhody - Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb;
- ISO/IEC 17000:2020 Posudzovanie zhody - Slovník a všeobecné zásady.

Pokiaľ nie je uvedená verzia dokumentu, všetky vyššie uvedené právne predpisy a technické normy sú citované v znení ich platnej verzie.

2.3 CERTIFIKAČNÉ ROLY

2.3.1 Vlastník certifikačnej schémy

Certifikačnú schému overovania odbornej spôsobilosti manažéra vydáva **Národný bezpečnostný úrad (NBÚ)**, ako orgán dohľadu v oblasti kybernetickej bezpečnosti. Certifikačná schéma stanovuje postup pri certifikácii manažéra kybernetickej bezpečnosti podľa osobitného predpisu.[2)]

2.3.2 Orgány posudzovania zhody

V záujme zachovania kvality určuje certifikačná schéma certifikačné procesy, všeobecné a osobitné požiadavky na certifikáciu manažéra kybernetickej bezpečnosti. Služby posudzovania zhody vykonávajú **orgány posudzovania zhody** podľa tejto certifikačnej schémy a podľa odporúčaní medzinárodne akceptovaných štandardov alebo iných vecne obdobných postupov[3)] príslušným na certifikáciu personálu.

Orgán posudzovania zhody vydávajúci certifikáty založené na tejto certifikačnej schéme musí spĺňať požiadavky medzinárodnej normy ISO/IEC 17024.

[1)] § 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.

[2)] Zákon č. 56/2018 Z. z. o posudzovaní zhody výrobku, sprístupňovaní určeného výrobku na trhu a o zmene a doplnení niektorých zákonov v znení zákona č. 259/2021 Z. z.

Orgán posudzovania zhody je oprávnený vydávať certifikát manažéra kybernetickej bezpečnosti podľa osobitného predpisu.[3)]

2.3.3 Akreditačný orgán

Vnútroštátny **akreditačný orgán** je jediný orgán v členskom štáte Európskej únie (EÚ), ktorý vykonáva akreditáciu na základe právomoci, ktorú mu udelil štát. V Slovenskej republike je vnútroštátnym akreditačným orgánom Slovenská národná akreditačná služba (SNAS). Postavenie SNAS a jej pôsobnosť určuje zákon č. 505/2009 Z. z. o akreditácii orgánov posudzovania zhody a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Orgán posudzovania zhody je oprávnený vydávať certifikát manažéra kybernetickej bezpečnosti len za predpokladu, že je na to akreditovaný Slovenskou národnou akreditačnou službou[3]) pre oblasť certifikácie manažérov v súlade s touto certifikačnou schémou.

[3]) § 9 zákona č. 505/2009 Z. z. o akreditácii orgánov posudzovania zhody a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

3 KRITÉRIÁ CERTIFIKÁCIE

3.1 VŠEOBECNÉ POŽIADAVKY NA SPÔSOBILOSŤ

3.1.1 Minimálne všeobecné požiadavky na spôsobilosť

Od kandidáta sa vyžaduje znalosť v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti, riadenia služieb informačných technológií (IT) a správy informačných systémov. Kandidát musí byť schopný analyzovať a riadiť systém manažérstva informačnej bezpečnosti v súlade s príslušnými technickými normami a právnymi predpismi a aplikovať príslušné metódy riadenia.

3.1.2 Minimálne požiadavky na vzdelanie a prax

Minimálne požiadavky na úroveň vzdelania a prax žiadateľa o overenie odbornej spôsobilosti:

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

3.1.3 Všeobecné predpoklady na výkon činnosti manažéra

Kandidátom sa môže stať fyzická osoba, ktorá:

- má spôsobilosť na právne úkony v plnom rozsahu,

- je bezúhonná – za buzúhonného sa na účely tejto schémy nepovažuje ten, kto bol v posledných 5 rokoch právoplatne odsúdený za niektorý z trestných činov uvedených v § 247 až § 247d zákona č. 300/2005 Z. z. Trestného zákona,
- spĺňa osobitné a všeobecné požiadavky na spôsobilosť.

3.1.4 Špecifické kľúčové kompetencie

Od kandidáta sa vyžadujú nasledujúce osobnostné požiadavky a schopnosti:

- schopnosť prijímať rozhodnutia,
- schopnosť myslieť a konať v súvislostiach,
- schopnosť riešiť konflikty,
- schopnosť poskytovať spätnú väzbu,
- schopnosť delegovať úlohy,
- schopnosť podporovať procesy vzdelávania a odovzdávania znalostí,
- schopnosť viesť pracovný tím,
- schopnosť organizovania a plánovania práce,
- analytické myslenie,
- strategické a koncepčné myslenie,
- tvorivosť (kreativita),
- prezentačná zručnosť.

3.2 OSOBITNÉ POŽIADAVKY NA SPÔSOBILOSŤ

Od kandidáta sa vyžadujú nasledujúce minimálne požiadavky - **vedomosti** na úroveň odbornej spôsobilosti manažéra pre proces riadenia kybernetickej bezpečnosti:

Pre oblasť riadenia bezpečnosti:

1. procesy, systémy a zásady riadenia kybernetickej bezpečnosti vrátane zásad riadenia fyzickej a objektovej bezpečnosti
2. organizácia kybernetickej bezpečnosti
3. terminológia a skratky v oblasti kybernetickej bezpečnosti
4. princípy riadenia IT služieb, správy systémov a správy počítačových sietí
5. hodnotiace a validačné kritériá v oblasti kybernetickej bezpečnosti (KPI, KRI atď.)
6. zdroje, charakteristiky a použitie informačných aktív organizácie
7. organizačné politiky, organizačné štruktúry a koncepty plánovania vzťahov s internými a/alebo externými organizáciami
8. koncepcie zlepšovania organizačných procesov a modely hodnotenia vyspelosti procesov (napr. CMMI)
9. zásady a techniky plánovania kapacity a plánovania zdrojov
10. princípy riadenia ľudských zdrojov
11. rozpočtové pravidlá, zásady plánovania a riadenia nákladov a plánovania a riadenia investícií
12. základy compliance v oblasti kybernetickej bezpečnosti (právny rámec aspoň na úrovni zákona o ITVS, GDPR, ePrivacy, ISO 20000)
13. výskumné stratégie a znalostný manažment
14. princípy podnikovej architektúry, koncepcie bezpečnostnej architektúry a referenčné modely podnikovej architektúry (napr. TOGAF, Zachman, FEA atď.)

15. koncepty, terminológia a princípy prevádzky elektronických komunikačných systémov (počítačové a telefónne siete, satelitné, optické, bezdrôtové atď.)
16. model OSI, mapovanie siete, topológia sietí, hlavné sieťové protokoly
17. princípy sieťových zariadení (rozbočovače, prepínače, smerovače, brány, firewall atď.)
18. zásady riadenia dodávateľských služieb a obstarávania informačných systémov vrátane vyhodnocovania dôveryhodnosti dodávateľa alebo výrobku

Pre oblasť riadenia hrozieb a rizík:

1. procesy riadenia rizík, postupy a metodiky analýzy rizík
2. typické kybernetické bezpečnostné hrozby a zraniteľnosti a metódy ich identifikácie
3. zásady aplikačnej bezpečnosti
4. teória, koncepty a metódy systémového inžinierstva
5. metódy a techniky softvérového inžinierstva vrátane modelov vývoja softvéru, princípy životného cyklu vývoja systémov a zásady bezpečného vývoja softvéru
6. bezpečnostné koncepty v operačných systémoch
7. bezpečnostné mechanizmy a metódy v softvérovom inžinierstve (napr. modularizácia, vrstvenie, abstrakcia, maskovanie, šifrovanie, pseudonymizácia, minimalizácia spracúvania atď.)
8. techniky a metódy riadenia konfigurácií a vplyv konfigurácií na bezpečnosť
9. nástroje na posudzovanie zraniteľností
10. sieťové protokoly a adresárové služby
11. základná architektúra operačných systémov (napr. riadenie systémových procesov, štruktúra adresárov, inštalácia a spúšťanie procesov a aplikácií)
12. bezpečnostné riziká cloud computingu
13. všeobecné koncepty operačných technológií a riadiacich systémov (OT/ICS)

Pre oblasť aplikácie bezpečnostných opatrení:

1. princípy navrhovania opatrení na ošetrenie bezpečnostných rizík
2. bezpečnostné mechanizmy a spôsob ich implementácie
3. bezpečnostné opatrenia vo fyzickej a objektovej bezpečnosti
4. nástroje, metódy a techniky navrhovania bezpečnostných systémov
5. zásady personálnej bezpečnosti
6. opatrenia týkajúce sa používania, spracúvania, uchovávania a prenosu údajov
7. zásady a princípy riadenia identít a prístupov
8. základy kryptografických bezpečnostných mechanizmov
9. koncepcie a technológie vzdialeného prístupu
10. základy virtualizačných technológií, vývoja a údržby virtuálnych strojov
11. princípy zabezpečenia virtuálnych privátnych sietí (VPN)
12. techniky a metódy správy systémov a hardeningu systémov

Pre oblasť výkonu operatívnych bezpečonstných činností:

1. procesy riešenia kybernetických bezpečnostných incidentov
2. zásady riadenia bezpečnosti prostredia cloudu
3. zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia
4. princípy logovania a bezpečnostného monitorovania
5. princípy korelácie bezpečnostných udalostí

6. základné postupy pri spracovaní digitálnych stôp
7. základy penetračného testovania

Pre oblasť riadenia súladu:

1. právne predpisy, požiadavky na súlad a technické normy vzťahujúce sa na kybernetickú bezpečnosť a ochranu osobných údajov
2. základy compliance v oblasti kybernetickej bezpečnosti (právny rámec aspoň na úrovni zákona o ITVS, GDPR, ePrivacy, ISO 20000)
3. požiadavky právnych predpisov na bezpečnostnú dokumentáciu a bezpečnostné politiky
4. princípy posudzovania kybernetickej bezpečnosti
5. politiky, procesy a postupy pre riadenie ľudských zdrojov v organizácii
6. systémy odbornej prípravy, princípy vzdelávacích stratégií, procesov a postupov vzdelávania a zvyšovania povedomia u dospelých v oblasti kybernetickej bezpečnosti vrátane merania efektivity vzdelávania
7. zásady a metódy tvorby učebných plánov, výuky jednotlivcov a skupín
8. štandardy bezpečnosti platobných kariet (PCI)
9. štandardy a procesy riadenia rizík v dodávateľskom reťazci
10. metódy testovania a vyhodnocovania bezpečnosti systémov

Od kandidáta sa vyžadujú nasledujúce minimálne požiadavky - **zručnosti** na úroveň odbornej spôsobilosti manažéra pre proces riadenia kybernetickej bezpečnosti:

Pre oblasť riadenia bezpečnosti:

1. strategické riadenie kybernetickej bezpečnosti organizácie
2. vypracovanie a prezentácia bezpečnostných stratégií a konceptov
3. implementácia a riadenie procesov kybernetickej bezpečnosti podľa všeobecne záväzných právnych predpisov, bezpečnostnej stratégie a ostatných interných riadiacich aktov
4. zabezpečenie, vypracovanie, udržiavanie a aktualizácie bezpečnostnej dokumentácie kybernetickej bezpečnosti a ďalších interných riadiacich aktov vo vzťahu k bezpečnosti organizácie
5. návrh požiadaviek na rozpočet a na iné zdroje súvisiace s bezpečnostnými opatreniami a procesmi relevantnými z hľadiska kybernetickej bezpečnosti vrátane riadenia nákladov a riadenia investícií
6. metodické usmerňovanie správcov a gestorov informačných a komunikačných technológií, vlastníkov procesov, vlastníkov aktív, vedúcich zamestnancov a ďalších zodpovedných zamestnancov vo vzťahu k dosahovaniu bezpečnostných cieľov organizácie
7. poskytovanie informácií bezpečnostnému výboru alebo štatutárnemu orgánu o stave kybernetickej bezpečnosti v organizácii, o závažných bezpečnostných rizikách, kybernetických bezpečnostných incidentoch a významných bezpečnostných udalostiach
8. riadenie kybernetickej bezpečnosti vo vzťahu s dodávateľmi a pri obstarávaní a vývoji softvéru a systémov

Pre oblasť riadenia hrozieb a rizík:

1. implementácia a manažment procesov identifikácie, analýzy a monitoringu bezpečnostných hrozieb a rizík
2. posudzovanie hrozieb a rizík
3. návrh opatrení na ošetrovanie rizík a na zamedzenie dopadov bezpečnostných udalostí
4. zabezpečovanie procesov hodnotenia technických zraniteľností systémov

5. manažment procesov detekcie, riešenia, evidencie a prevencie kybernetických bezpečnostných incidentov
6. zabezpečenie funkčných plánov kontinuity a obnovy činností organizácie
7. koordinácia a riadenie procesov obnovy prevádzkových činností (tzv. Business Continuity Management) vrátane riadenia procesov plánovania obnovy systémov po havárii (tzv. Disaster Recovery Planning)

Pre oblasť aplikácie bezpečnostných opatrení:

1. riadenie návrhov, implementácie, zmien a optimalizácie bezpečnostných riešení s víziou a konceptom ich bežného prevádzkovania
2. zabezpečovanie implementácie technických a organizačných bezpečnostných opatrení
3. riadenie bezpečnostnej architektúry
4. predkladanie odborných stanovísk k novým zmenám v IT infraštruktúre, ktoré môžu mať potenciálny vplyv na bezpečnosť informačných aktív organizácie
5. monitorovanie plnenia a efektivity bezpečnostných mechanizmov a opatrení

Pre oblasť výkonu operatívnych bezpečnostných činností:

1. manažment výkonu činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe
2. vedenie tímu zamestnancov útvaru informačnej a kybernetickej bezpečnosti, ak je taký organizačný útvar zriadený
3. návrh a aplikácia metodík pre klasifikáciu informačných aktív a kategorizáciu sietí a informačných systémov
4. riadenie bežnej prevádzky technických bezpečnostných opatrení
5. zabezpečovanie udržateľnosti organizačných opatrení vrátane vyspelosti bezpečnostných procesov
6. zaistenie uplatňovania princípu oddelenia právomocí a zodpovedností v celej organizačnej štruktúre organizácie
7. základy projektového manažmentu

Pre oblasť riadenia súladu:

1. riadenie procesov zaručenia súladu (Compliance Management) v oblasti kybernetickej bezpečnosti
2. zabezpečenie pravidelného preskúmavania stavu kybernetickej a informačnej bezpečnosti
3. vyhodnocovanie plnenia vnútorných predpisov súvisiacich s riadením kybernetickej bezpečnosti
4. poskytovanie súčinnosti internému a externému auditu kybernetickej bezpečnosti
5. navrhovanie metrík a kľúčových indikátorov pre sledovanie vývoja a stavu bezpečnosti a vývoja bezpečnostných rizík
6. zabezpečovanie školení zamestnancov v oblasti kybernetickej bezpečnosti
7. zabezpečovanie kontinuálneho vzdelávania pre pracovné roly relevantné z hľadiska kybernetickej bezpečnosti
8. zabezpečovanie budovania bezpečnostného povedomia pre oblasť informačnej a kybernetickej bezpečnosti a ochrany osobných údajov
9. spolupráca s orgánmi verejnej moci a orgánmi činnými v trestnom konaní

4 POSÚDENIE ZHODY

Posúdenie spôsobilosti kandidátov podľa tejto schémy má za cieľ overiť a potvrdiť, že boli dosiahnuté požiadavky na kvalifikáciu manažéra kybernetickej bezpečnosti podľa podľa vyhlášky č. 492/2022 Z. z. s príslušnými spôsobilosťami, ktoré umožnia manažérom kybernetickej bezpečnosti samostatne riadiť kybernetickú bezpečnosť v organizácii, riadiť implementáciu a udržiavanie opatrení v súlade s požiadavkami vyhlášky č. 362/2018 Z. z.

4.1 POČIATOČNÉ KRITÉRIÁ CERTIFIKÁCIE

Ako predpoklad počiatočnej certifikácie musí orgán posudzovania zhody vyžadovať objektívne dôkazy o tom, že osoba, ktorá žiada o certifikáciu, spĺňa základné požiadavky týkajúce sa profilu uvedené v príslušnej špecifikácii spôsobilosti. Každý orgán posudzovania zhody je zodpovedný za identifikáciu vhodných referenčných úrovní v rámci príslušného kontextu národnej kvalifikácie a odbornej prípravy.

Predpoklady počiatočnej certifikácie zahŕňajú najmä:

- príslušné vzdelanie,
- prax a rozsah všeobecných pracovných skúseností,
- formálne školenia a odborné certifikáty,
- manažérske skúsenosti,
- plnenie požiadaviek kódexu profesionálneho správania manažéra kybernetickej bezpečnosti (etický kódex).

v kontexte systému hodnotenia a certifikácie riadeného v súlade s pravidlami akreditačného orgánu v členskom štáte EÚ, pod dohľadom akreditačného orgánu členského štátu.

Osvedčenia, ktorými je potvrdená atestácia splnenia všetkých týchto podmienok, sa na účely tejto schémy nazývajú „certifikáty“.

4.2 POSUDZOVANIE ŽIADATEĽOV

Posúdenie sa vykonáva plánovaným a štruktúrovaným spôsobom, ktorý zabezpečí, aby požiadavky schémy boli objektívne a systematicky overené a boli písomne dokumentované dôkazy potvrdzujúce kompetentnosť kandidáta.

Vlastník certifikačnej schémy priebežne overuje účinnosť metód na posudzovanie žiadateľov. Týmto overením sa zabezpečí, aby každé posúdenie bolo spravodlivé a platné.

Konkrétne hodnotiace kritériá a metódy, ktoré sa majú použiť, vrátane druhov hodnotenia, s cieľom preukázať, že sa dosiahli požadované ciele, môžu byť predmetom samostatných metodických usmernení vlastníka certifikačnej schémy.

4.3 ODBORNÁ SKÚŠKA

4.3.1 Obsah odbornej skúšky

Odborná skúška manažéra kybernetickej bezpečnosti sa vykonáva zo znalosti všeobecne záväzných právnych predpisov upravujúcich kybernetickú bezpečnosť a ochranu kritickej infraštruktúry v kontexte informačných a komunikačných technológií a oblastí spôsobilostí uvedených v kapitole 3.2.

Odborná skúška je vykonávaná formou testu obsahujúceho 100 otázok zo znalosti všeobecne záväzných právnych predpisov a príslušných technických noriem o podmienkach výkonu činnosti manažéra kybernetickej bezpečnosti a o bezpečnostných opatreniach v kybernetickej bezpečnosti. Konkrétny rozsah otázok je riešený v nasledujúcom článku tejto schémy.

Pre každú skúšku sa vygeneruje **100 otázok** náhodným výberom zo súboru obsahujúceho najmenej **400 otázok** schválených vlastníkom certifikačnej schémy.

Návrh každej skúšobnej otázky obsahuje:

a) znenie skúšobnej otázky, alebo príkladu s jednoznačným zadaním úlohy,
b) návrh štyroch alternatívnych odpovedí pre danú otázku, z ktorých len jedna odpoveď môže byť správna,
c) označenie správnych a nesprávnych odpovedí,
d) vymedzenie odbornej domény, do ktorej príslušný návrh otázky patrí,
e) návrh bodového ohodnotenia otázky,
f) voliteľne – komentár ku spôsobu riešenia navrhnutej otázky.

Každá otázka má 4 možnosti odpovedí, pričom správna je len jedna odpoveď. **Časový rozsah skúšky na 100 otázok je 150 minút** (t.j. 1,5 min./otázka).

Národný bezpečnostný úrad ako vlastník certifikačnej schémy na svojom webovom sídle zverejňuje okruhy a príklady otázok na vykonanie odbornej skúšky a usmernenie na ich používanie.

4.3.2 Požiadavky na skúšobné otázky

Každý orgán posudzovania zhody uchováva skúšobné otázky / prípadové štúdie / scenáre pre potreby odbornej skúšky. Štruktúra a obsah množiny otázok sa vzťahuje na vedomosti a zručnosti definované v platnej špecifikácii spôsobilostí.

Pre každú odbornú skúšku musí byť k dispozícii trojnásobný počet otázok vybratých pre skúšku. Otázky musia byť vyberané tak, aby sa zabezpečila nezávislosť jednotlivých skúšok.

Okruhy skúšobných otázok musia obsahovať otázky z nasledujúcich odborných domén:

a) Riadenie kybernetickej a informačnej bezpečnosti
b) Riadenie IT služieb
c) Riadenie prístupov
d) IT architektúra
e) Riadenie aktív, hrozieb a rizík
f) Vývoj systémov (SDLC)
g) Riadenie tretích strán a dodávateľských služieb
h) Bezpečnosť prevádzky IT
i) Bezpečnosť počítačových sietí
j) Riešenie incidentov
k) Manažment bezpečnostných zraniteľností
l) Základy bezpečnosti OT/ICS/SCADA
m) Personálna bezpečnosť
n) Riadenie kontinuity
o) Strategický manažment
p) Legislatíva a štandardy

4.3.3 Príprava otázok na odbornú skúšku

Za prípravu otázok na odbornú skúšku manažéra kybernetickej bezpečnosti je zodpovedný orgán posudzovania zhody.

Množina skúšobných otázok musí byť najmenej 30 dní pred ich zaradením do procesu skúšky predložená vlastníkovi certifikačnej schémy na schválenie. Vlastník certifikačnej schémy má výhradné právo na zmenu,

pridanie, alebo odstránenie akejkoľvek otázky z množiny navrhnutých skúšobných otázok. Vlastník certifikačnej schémy sa ku predloženým otázkam vyjadrí najneskôr v lehote do 15 dní. Po schválení množiny otázok vlastníkom certifikačnej schémy, môže orgán posudzovania zhody danú množinu otázok používať v procese skúšky. Orgán posudzovania zhody zabezpečí, aby sa neplatné verzie množín otázok uchovávali v archíve po dobu 3 rokov.

4.3.4 Kvalifikačné požiadavky na skúšajúcich

Skúšajúci musí spĺňať nasledujúce kvalifikačné predpoklady:

- schopnosť plynulo a zrozumiteľne komunikovať v slovenskom alebo českom jazyku,
- ovládanie procesov skúšky, jej priebehu a vyhodnotenia,
- ovládanie technických testovacích prostriedkov (pre dištančnú / online formu skúšky),
- znalosť problematiky, ktorá je predmetom skúšky,
- spoľahlivosť a nestrannosť.

4.3.5 Termín a miesto vykonania odbornej skúšky

Termín, miesto a metódu vykonania odbornej skúšky určuje orgán posudzovania zhody.

Pozvánka na odbornú skúšku sa doručuje žiadateľovi v elektronickej podobe najneskôr 15 dní pred termínom konania skúšky.

Ak sa žiadateľ na skúšku nedostaví, ale vopred sa ospravedlní, je automaticky zaradený a pozvaný na najbližší voľný termín.

V prípade, že sa žiadateľ nedostaví ani na náhradný termín odbornej skúšky, orgán posudzovania zhody môže navrhnúť vyradenie tohto žiadateľa zo zoznamu žiadateľov. Vyradenie žiadateľa podlieha schváleniu vedúcim certifikačného orgánu.

Ak kandidát nebol na skúške úspešný, môže sa po obdržaní rozhodnutia o skúške prihlásiť na ďalší voľný termín skúšky. Početnosť opakovaní skúšky nie je limitovaná.

4.3.6 Priebeh odbornej skúšky

Test sa vykonáva písomnou formou, a to buď prezenčne alebo dištančne za použitia vhodných technických prostriedkov. O spôsobe vykonania testu musia byť kandidáti informovaní v pozvánke na skúšku.

Priebeh odbornej skúšky riadi skúšajúci podľa postupu Pokyny pre skúšajúcich a metodika skúšky, ktoré obsahujú aj postup na vyhodnotenie skúšky.

Pred začatím odbornej skúšky kandidát preukáže svoju totožnosť dokladom totožnosti a orgán posudzovania zhody ho poučí o pravidlách priebehu skúšky. Ak kandidát pred začatím odbornej skúšky nepreukáže svoju totožnosť alebo sa počas skúšky správa v rozpore s pravidlami priebehu skúšky a dobrými mravmi, skúšajúci rozhodne o vylúčení kandidáta zo skúšky a hľadí sa na neho akoby skúšku vykonal neúspešne. Vylúčenie kandidáta zo skúšky musí byť skúšajúcim písomne odôvodnené.

Kandidát je po celý čas prípravy a priebehu odbornej skúšky, ktorá sa vykonáva dištančnou formou, monitorovaný použitím video konferenčných nástrojov. V prípade pokynu skúšajúceho je kandidát povinný preukázať, že v miestnosti sa nenachádza iná osoba.

4.3.7 Vyhodnotenie odbornej skúšky

Skúšajúci vyhodnotí správnosť odpovedí. V prípade písomne vykonávanej skúšky prostredníctvom pripravenej šablóny správnych odpovedí, správne odpovede vyznačí zakrúžkovaním čísla otázky.

V prípade skúšky vykonanej dištančne za použitia technických prostriedkov sú odpovede vyhodnotené pomocou reportovacej funkcie softvérového testovacieho nástroja.

Kandidát sa považuje za **úspešného**, ak v skúške dosiahne **najmenej 55%** správnych odpovedí.

Kandidát sa považuje za **neúspešného**, ak v skúške dosiahne v hodnotení **menej ako 55%** správnych odpovedí.

Dokumentácia priebehu a výsledkov odbornej skúšky, testovacie otázky, vyhodnotenia testov a štatistiky úspešnosti nie sú kandidátom sprístupňované.

Sťažnosti na priebeh skúšky alebo vyhodnotenie skúšky, vrátane odvolaní proti vyhodnoteným výsledkom sa vybavujú v zmysle postupu uvedeného v kapitole 6.

5 CERTIFIKÁT

5.1 UDELENIE CERTIFIKÁTU

Podkladmi pre vydanie certifikátu manažéra kybernetickej bezpečnosti je splnenie všeobecných požiadaviek na spôsobilosť podľa tejto certifikačnej schémy **a výsledky odbornej skúšky**. Certifikát vydáva kompetentná osoba v súlade s požiadavkami na orgán posudzovania zhody podľa technickej normy[4)] a v súlade s touto certifikačnou schémou.

Platnosť certifikátu manažéra kybernetickej bezpečnosti sa začína dňom vydania certifikátu manažéra kybernetickej bezpečnosti, ktorý je svojim označením totožný s dňom uvedeným na rozhodnutí o udelení certifikátu manažéra kybernetickej bezpečnosti. Certifikát manažéra kybernetickej bezpečnosti sa doručuje elektronicky alebo poštou, alebo si ho môže manažér kybernetickej bezpečnosti na základe vlastnej žiadosti prevziať osobne.

Doba platnosti certifikátu manažéra kybernetickej bezpečnosti je **3 roky od jeho vydania**. Manažér kybernetickej bezpečnosti počas doby platnosti certifikátu manažéra kybernetickej bezpečnosti využíva svoj certifikát manažéra v súlade s podmienkami a obmedzeniami v ňom uvedenými, poskytuje na vyžiadanie súčinnosť orgánu posudzovania zhody a zaväzuje sa poskytnúť mu pravdivé informácie a dokumenty vyžadované touto schémou. Svoju činnosť vykonáva manažér kybernetickej bezpečnosti odborne a v súlade s dobrými mravmi.

5.2 DOHĽAD NAD ČINNOSŤOU CERTIFIKOVANÉHO MANAŽÉRA

Posudzovanie zhody sa môže skončiť vydaním vyhlásenia, vo forme certifikátu manažéra kybernetickej bezpečnosti. V prípade osobitného zreteľa alebo osobitnej povahy je certifikačný orgán oprávnený vykonať mimoriadny dohľad, ktorého cieľom je potvrdiť alebo vyvrátiť prípadne pochybnosti o plnení stanovených touot schémou.

O vykonaní mimoriadneho dohľadu nad činnosťami vykonávanými certifikovanými manažérmi kybernetickej bezpečnosti písomne rozhodne vedenie orgánu posudzovania zhody. Rozhodnutie môže byť vykonané na základe:

- vlastného rozhodnutia v prípade, že sa podmienky posúdenia objektu posudzovania zhody časom zmenili, čo by mohlo ovplyvniť pokračujúce plnenie požiadaviek tejto schémy
- žiadosti objektu posudzovania zhody, ktorý si vyžaduje ďalšie preukázanie, že požiadavky sa skutočne plnia,
- obdržanej sťažnosti na činnosť manažéra kybernetickej bezpečnosti, alebo na základe informácie o možnom porušovaní povinností podľa tejto certifikačnej schémy.

V rámci dohľadu sa môže vykonať:

- pohovor s manažérom kybernetickej bezpečnosti s cieľom zistiť jeho znalosti a zručnosti, zvyšovanie znalostí absolvovaním kurzov a pod.,
- kontrola záznamov manažéra kybernetickej bezpečnosti o sťažnostiach zainteresovaných strán, sťažnostiach Národného bezpečnostného úradu, ich vybavenie, nápravné opatrenia a ich účinnosť,
- zaslanie upozornení certifikovaným manažérom zo strany orgánu posudzovania zhody na prípadné porušenia alebo iné zistenia, ktoré by mohli byť v rozpore s etickým kódexom certifikovaného manažéra, certifikačnými požiadavkami orgánu posudzovania zhody alebo požiadavkami certifikačnej schémy.

[4)] ISO/IEC 17024:2012 Posudzovanie zhody - Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb.

V odôvodnených prípadoch sa môže pri dohľade vykonať posúdenie vlastného výkonu riadenia kybernetickej bezpečnosti. Na tento účel orgán posudzovania zhody využíva len vlastných zamestnancov, ktorí sú viazaní mlčanlivosťou pri danom výkone posúdenia voči posudzovanému subjektu. O vykonanom dohľade spracuje orgán posudzovania zhody zápis, ktorý okrem zistených skutočností obsahuje aj termín predloženia nápravných opatrení na odstránenie zistených nedostatkov. Zápis orgán posudzovania zhody prerokuje s certifikovaným manažérom kybernetickej bezpečnosti, ktorý svojim podpisom potvrdí oboznámenie sa s protokolom, a ak s niektorými závermi nesúhlasí, uvedie svoje stanovisko (námietky, zdôvodnenie nesúhlasu). Záznamy z dohľadov sa evidujú v spise manažéra. Výkonom takéhoto posúdenia certifikovaný manažér neporušil žiadnu povinnosť mlčanlivosti.

5.3 OBNOVA CERTIFIKÁTU A PREDĹŽENIE PLATNOSTI CERTIFIKÁTU

5.3.1 Obnova platnosti certifikátu manažéra

O obnovu certifikátu manažéra kybernetickej bezpečnosti možno požiadať aj pred uplynutím doby platnosti aktuálne platného certifikátu manažéra:

a) ak to vyplýva zo všeobecne záväzných právnych predpisov,
b) na základe zmeny požiadaviek certifikačnej schémy,
c) vzhľadom na povahu a rozvinutosť priemyslu alebo odvetvia, v ktorom manažér pôsobí,
d) vzhľadom na prebiehajúce zmeny v technológiách a požiadavkách na manažérov alebo
e) na základe odôvodnenej požiadavky zainteresovaných strán.

Na žiadosť, konanie a na vydanie certifikátu manažéra kybernetickej bezpečnosti a na certifikát manažéra kybernetickej bezpečnosti sa vzťahujú ustanovenia o certifikácii manažéra kybernetickej bezpečnosti a certifikačná schéma.

5.3.2 Predĺženie platnosti certifikátu manažéra

Pred uplynutím doby platnosti certifikátu manažéra kybernetickej bezpečnosti môže manažér kybernetickej bezpečnosti požiadať o predĺženie platnosti svojho certifikátu manažéra na ďalšie trojročné obdobie. Žiadosť sa podáva najneskôr tri mesiace pred skončením platnosti certifikátu manažéra kybernetickej bezpečnosti. O výnimkách z požiadaviek na dodržanie lehôt manažérmi, rozsahu a forme poskytnutých podkladov v individuálnych prípadoch rozhoduje orgán posudzovania zhody. Uplatnenie každej výnimky musí byť písomne zdôvodnené a nesmie byť v rozpore s touto certifikačnou schémou.

Podmienkou pre vydanie nového certifikátu manažéra kybernetickej bezpečnosti je, že manažér kybernetickej bezpečnosti:

a) počas doby platnosti certifikátu spĺňa podmienky certifikácie a
b) preukáže, že:
   - si udržiava vedomosti a prax: udržiavanie praktických zručností doložením výkonu praxe manažéra kybernetickej bezpečnosti u prevadzkovateľa základnej služby počas doby platnosti certifikátu (orgán posudzovania zhody je oprávnený preveriť pravdivosť výkonu činností manažéra kybernetickej bezpečnosti, a to prostredníctvom informácií o prevádzkovateľovi základnej služby doložených certifikovaným manažérom: obdobie výkonu činností manažéra kybernetickej bezpečnosti, názov organizácie, overiteľná referencia – meno/pozícia, telefónne číslo),
   - si zvyšuje kvalifikáciu v oblasti kybernetickej bezpečnosti najmenej v rozsahu absolvovania 60 hodín odborného vzdelávania v informačnej a kybernetickej bezpečnosti počas doby platnosti certifikátu,
   - je nezávislý a predchádza konfliktu záujmov (dokladá sa čestným prehlásením, nezávislosť a predchádzanie konfliktu záujmov musí byť dodržané počas celého obdobia platnosti certifikátu).

Zvyšovanie kvalifikácie pozostáva najmä z:

- účasti na školeniach, konferenciách a webinároch v oblasti kybernetickej bezpečnosti (doložením rozsahu podujatia v hodinách),
- samoštúdiom odbornej literatúry v rozsahu max. 20 hodín ročne (dokladuje sa čestným prehlásením a zoznamom odbornej literatúry),
- publikačnej činnosti (každá normostrana publikácie sa akceptuje ako jedna hodina),
- prednáškovej činnosti (akceptuje sa jedna hodina za každú odprednášanú hodinu, na prípravu prednášky je možné započítať päťnásobok času prednášania pri jedinečnom obsahu prednášky a jedennásobok času prednášania pri opakovanom prednášaní prednášky).

5.3.3 Zmena predmetu certifikácie

Certifikačná schéma v tejto verzii nepredpokladá zavedenie rôznych úrovní certifikácie, ani zmenu predmetu certifikácie.

5.4 POZASTAVENIE ALEBO ZRUŠENIE CERTIFIKÁTU MANAŽÉRA

Pozastavenie platnosti certifikátu manažéra môže nastať rozhodnutím orgánu posudzovania zhody na základe podnetu NBÚ, alebo na základe požiadania manažéra kybernetickej bezpečnosti.

5.4.1 Pozastavenie alebo zrušenie platnosti certifikátu orgánom posudzovania zhody

Orgán posudzovania zhody môže pozasaviť alebo zrušiť platnosť certifikátu manažéra kybernetickej bezpečnosti v nasledujúcich prípadoch:

- certifikovaná osoba nespĺňa všeobecné predpoklady na výkon činnosti manažéra (bod 3.1.3 tejto schémy);
- certifikovaná osoba preukázateľne nedodržiava etický kódex;
- certifikovaný manažér kybernetickej bezpečnosti dobrovoľne požiada o pozastavenie alebo zrušenie platnosti certifikátu.

Orgán posudzovania zhody je povinný tieto okolnosti prešetriť a prijať príslušné opatrenia. Ak nedôjde v lehote určenej orgánom posudzovania zhody, ktorá nesmie byť kratšia ako 30 dní, k náprave skutočností, ktoré viedli k pozastaveniu platnosti certifikátu manažéra kybernetickej bezpečnosti, orgán posudzovania zhody ukončí platnosť vydaného certifikátu manažéra kybernetickej bezpečnosti.

Certifikačný orgán vymedzí a oznámi postup pozastavenia a zrušenia certifikátu manažéra kybernetickej bezpečnosti.

5.4.2 Pozastavenie platnosti certifikátu na základe podnetu NBÚ

Orgán posudzovania zhody pozastaví platnosť certifikátu manažéra kybernetickej bezpečnosti na základe podnetu Národného bezpečnostného úradu pri porušovaní povinností podľa tejto certifikačnej schémy.

Platnosť certifikátu môže byť rozhodnutím orgánu posudzovania zhody pozastavená **na dobu najviac 90 dní**. Orgán posudzovania zhody bezodkladne písomne vyzve manažéra kybernetickej bezpečnosti k náprave skutočností, ktoré viedli k pozastaveniu platnosti certifikátu manažéra kybernetickej bezpečnosti.

Ak nedôjde v lehote určenej orgánom posudzovania zhody, ktorá nesmie byť kratšia ako 30 dní, k náprave skutočností, ktoré viedli k pozastaveniu platnosti certifikátu manažéra, orgán posudzovania zhody ukončí platnosť vydaného certifikátu manažéra kybernetickej bezpečnosti.

5.4.3 Pozastavenie platnosti certifikátu na základe požiadavky manažéra kybernetickej bezpečnosti

Orgán posudzovania zhody pozastaví platnosť certifikátu manažéra kybernetickej bezpečnosti na základe písomnej požiadavky manažéra kybernetickej bezpečnosti. Takéto pozastavenie platnosti certifikátu manažéra kybernetickej bezpečnosti je možné len na dobu určitú, **maximálne však na 1 rok**, z nasledujúcich dôvodov:

- dlhodobej neprítomnosti,

- zo zdravotných dôvodov, alebo
- z dôvodov hroziaceho konfliktu záujmov.

Po uplynutí doby definovanej držiteľom certifikátu orgán posudzovania zhody obnoví platnosť vydaného certifikátu manažéra kybernetickej bezpečnosti.

5.4.4 Ukončenie platnosti certifikátu

Orgán posudzovania zhody môže ukončiť platnosť vydaného certifikátu manažéra kybernetickej bezpečnosti na základe:

- písomnej požiadavky manažéra kybernetickej bezpečnosti,
- nesplnenia požiadavky na nápravu skutočností, ktoré viedli k pozastaveniu platnosti certifikátu manažéra kybernetickej bezpečnosti v určenej lehote.

Orgán posudzovania zhody uzatvorí s manažérom kybernetickej bezpečnosti dohodu o zdržaní sa používania všetkých odkazov na certifikovaný status manažéra kybernetickej bezpečnosti, ak sa zruší platnosť certifikátu manažéra kybernetickej bezpečnosti.

6 VYBAVOVANIE SŤAŽNOSTÍ

Sťažnosti na priebeh skúšky alebo vyhodnotenie skúšky, vrátane odvolaní proti vyhodnoteným výsledkom a sťažnosti na výkon činnosti manažéra kybernetickej bezpečnosti spracúva a rieši orgán posudzovania zhody podľa technickej normy[4)] a v zmysle platnej politiky.

Orgán posudzovania zhody je povinný na svojom webovom sídle zverejniť záväznú politiku, ktorou:

- špecifikuje postupy pre vybavovanie sťažností a odvolaní v rámci procesov certifikácie,
- špecifikuje postupy pre vybavovanie sťažností na výkon činností manažéra,
- stanovuje zodpovednosti a zásady riešenia sporov.

7 VEDENIE EVIDENCIÍ

Orgán posudzovania zhody vedie evidenciu:

a) žiadostí o vydanie certifikátu manažéra kybernetickej bezpečnosti,
b) dokumentácie priebehu a výsledkov odbornej skúšky,
c) dokladov preukazujúcich splnenie podmienok podľa certifikačnej schémy,
d) vydaných certifikátov manažéra kybernetickej bezpečnosti,
e) iných súvisiacich dokumentov.

8 PRÍSTUP K CERTIFIKAČNEJ SCHÉME

Certifikačná schéma je verejný dokument, ktorý zverejňuje Národný bezpečnostný úrad na svojom webovom sídle.

V prípade pokrytia tejto certifikačnej schémy manažéra kybernetickej bezpečnosti akreditáciou SNAS, vlastník certifikačnej schémy je povinný informovať SNAS o zmenách certifikačnej schémy.

Dokumenty preukazujúce akreditáciu, resp. dokumenty súvisiace s certifikačným procesom (napr. akreditáciu, záväzné politiky, vzory zmlúv, atď.) zverejňuje orgán posudzovania zhody na svojom webom sídle, v nadväznosti na zmeny certifikačnej schémy.

Etický kódex manažéra kybernetickej bezpečnosti

Úvod

- Tento etický kódex je určený na podporu etického a profesionálneho správania vo všetkých oblastiach riadenia kybernetickej bezpečnosti. I keď znenie kódexu nie je odvodené od konkrétneho systému manažérstva, témy, ktoré obsahuje, sa týkajú najmä oblasti odbornej činnosti pracovnej roly manažéra kybernetickej bezpečnosti.
- Etický kódex má byť uplatniteľný pre rolu manažéra kybernetickej bezpečnosti všeobecne, v širokom spektre odvetví a typov organizácií.
    - V nasledujúcom texte kódexu je podľa pravidiel slovenského pravopisu na spoločné označenie mužských aj ženských reprezentantov profesie používané tzv. generické maskulínum, a forma mužského rodu je chápaná ako všeobecná, označujúca reprezentantov oboch pohlaví.

Profesijná zodpovednosť

- V reakcii na rýchle zmeny právneho, technologického a ekonomického prostredia, naberá v poslednej dobe pri výkone povolania manažéra kybernetickej bezpečnosti jeho ďalšie vzdelávanie na význame. Manažér kybernetickej bezpečnosti využije svoje odborné zručnosti, vedomosti a úsudok za všetkých okolností legálne, čestne a bezúhonne, s cieľom splnenia oprávnených záujmov zainteresovaných strán, ktorými môžu byť zákazníci, zamestnávatelia, alebo zákazníci zamestnávateľa.
- V súlade s náležitým dodržiavaním zákonných ustanovení a zásad výkonu povolania, musí manažér kybernetickej bezpečnosti vždy konať v najlepšom záujme zákazníka, alebo zamestnávateľa. Záujem zákazníka, alebo zamestnávateľa je povinný povýšiť nad vlastné záujmy a nad záujmy ostatných manažérov kybernetickej bezpečnosti.
- Manažér kybernetickej bezpečnosti podnikne všetky kroky na rozvoj vlastnej odbornej spôsobilosti v súlade s aktuálnym vývojom v profesionálnej oblasti.
- Manažér kybernetickej bezpečnosti si uplatní nárok iba na také členstvá a kvalifikácie, ktoré sú v danom čase platné.
- Manažér kybernetickej bezpečnosti sa zaväzuje vykonávať profesijnú činnosť odborne, objektívne, nestranne a v súlade s príslušnými všeobecne záväznými právnymi predpismi Slovenskej republiky, technickými normami a všeobecne uznávanou najlepšou praxou.
- Manažér kybernetickej bezpečnosti musí za každých okolností konať tak, aby zachoval dôstojnosť a dobrú povesť tejto profesie.
- Manažér kybernetickej bezpečnosti nebude vedome vykonávať činnosť, pre ktorú nemá dostatočné zručnosti, vedomosti a zodpovedajúcu právomoc.
- Akákoľvek reklama výkonu činnosti manažéra kybernetickej bezpečnosti musí byť slušná, legálna, čestná a vecná a nesmie byť vykonávaná ako porovnávanie s konkurenčnými činnosťami a službami.

Zodpovednosť voči klientom, zákazníkom a zamestnávateľom

- Manažér kybernetickej bezpečnosti musí poskytovať zákazníkom, zamestnávateľovi, alebo zákazníkom zamestnávateľa také odborné služby, ktoré sú profesionálne, objektívne, relevantné a včasné, spolu s príslušnými výhradami, alebo upozorneniami.
- Manažér kybernetickej bezpečnosti sa vyhýba takým činnostiam alebo úlohám, ktoré môžu spôsobiť konflikt záujmov pri výkone jeho pracovných zodpovedností.

- Manažér kybernetickej bezpečnosti je povinný zachovať mlčanlivosť vo vzťahu ku všetkým informáciám, získaným a poskytnutým počas profesijnej činnosti. Povinnosť zachovávať mlčanlivosť nie je časovo obmedzená. Povinnosť mlčanlivosti sa nevzťahuje na také informácie, u ktorých bolo preukázané, že sú alebo sa stali známymi bez zavinenia manažéra kybernetickej bezpečnosti ani na informácie, ktoré majú zmluvné strany povinnosť zverejniť v zmysle platných a účinných právnych predpisov Slovenskej republiky.
- Manažér kybernetickej bezpečnosti musí dodržiavať všetky potrebné a primerané opatrenia, aby zabránil vyzradeniu, zneužitiu, poškodeniu, zničeniu, strate alebo odcudzeniu, neoprávnenému prístupu, zmene a rozširovaniu informácií, údajov a dokladov, ktoré získal pri výkone činnosti manažéra kybernetickej bezpečnosti.
- Manažér kybernetickej bezpečnosti nesmie zneužívať svoje postavenie, súvisiace s výkonom jeho činnosti pri uskutočňovaní súkromných záujmov vo vlastný prospech alebo v prospech tretích strán.
- Certifikovaný manažér kybernetickej bezpečnosti je povinný bezodkladne oznámiť orgánu posudzovania zhody akékoľvek okolnosti, ktoré môžu mať potenciálne vplyv na jeho spôsobilosť, schopnosť alebo možnosť naďalej plniť certifikačné požiadavky (napr. prekážky v dodržiavaní kvalifikačných predpokladov, prerušenie celoživotného vzdelávania, odobratie alebo skončenie platnosti odborných certifikátov, zdravotné obmedzenia, osobné prekážky a pod.).

Zodpovednosť voči podriadeným a kolegom

- Manažér kybernetickej bezpečnosti musí zaručiť primeraný dohľad nad osobami, pracujúcimi v rámci jeho riadiacich právomocí alebo pod jeho dozorom a musí ich povzbudzovať v rozvoji ich odborných spôsobilostí.
- Manažér kybernetickej bezpečnosti sa vyhýba neodôvodnenej negatívnej komunikácii alebo publikovaniu neprimeranej kritiky, v súvislosti s odbornou činnosťou iného manažéra kybernetickej bezpečnosti.
- Manažér kybernetickej bezpečnosti nesmie úmyselne dostať kolegu - manažéra kybernetickej bezpečnosti do situácie, v ktorej by mohol nevedomky porušiť niektorú časť tohto etického kódexu.