Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Manažerské shrnutí

Vyhláška o inspektorech coby prováděcí právní předpis k novému Zákonu o kybernetické bezpečnosti bude ve upravovat a obsahovat v detailu to, jaké jsou nároky a požadavky na inspektora, jak se fyzická osoba může inspektorem stát a jak probíhá kontrola poskytovatele regulované služby v režimu nižších povinností vykonávaná inspektorem. Obsah uvedené vyhlášky by na základě toho měl být rozdělen do tří hlav, tak jak jsou specifikovány níže. ***Hlava první*** *vychází z § X [Inspektoři] nového Zákona o kybernetické bezpečnosti a stanovuje požadavky kladené na inspektory, které musí osoba naplňovat po celou dobu udělené autorizace. Konkrétně pak uvádí definici bezúhonnosti pro potřeby zákona a stanovuje požadavky na odbornou způsobilost, vzdělání a praxi. V případě, že inspektor přestane splňovat podmínky pro udělení autorizace upravené v této hlavě, bude mu autorizace rozhodnutím Úřadu odebrána (upraveno v § X [Inspektoři] odst. 9 nového Zákona o kybernetické bezpečnosti). Na ustanovení hlavy první dále navazuje příloha vyhlášky obsahující vzor žádosti fyzické osoby o udělení autorizace Úřadem. Součástí požadavků pro udělení autorizace je rovněž úspěšné složení zkoušky inspektora. V této hlavě je proto stanoven vlastní průběh a pravidla (počet otázek, časový rozsah zkoušky, zkušební okruhy, termíny vykonání zkoušky, předpoklady řádného složení, výše poplatku za umožnění složení zkoušky atd.) pro zkoušky potřebné k prokázání odborných znalostí. Na ustanovení týkající se zkoušky navazuje příloha vyhlášky obsahující minimální požadavky na odbornou způsobilost inspektora.* ***Hlava druhá*** *vychází z § X [Kontrola vykonávaná inspektory] a z § X [Pravidla pro výkon kontroly vykonávané inspektorem na vlastní žádost]nového Zákona o kybernetické bezpečnosti a stanovuje způsob výběru inspektora v případě jeho ustanovení ke kontrole rozhodnutím Úřadu, způsob určení délky trvání kontroly a zároveň specifikuje harmonogram výkonu kontroly. Na ustanovení hlavy třetí v tomto směru navazuje příloha vyhlášky obsahující tabulku pro výpočet dní trvání kontroly.* ***Hlava třetí*** *vychází z § X [Povinnosti inspektora] nového Zákona o kybernetické bezpečnosti a rozvíjí tak požadavky kladené na výkon kontroly, které musí inspektor během své činnosti naplňovat. Jedná se o standardní požadavky kladené na činnost auditorů. Činnost inspektorů je svým charakterem srovnatelná s činností auditorů a proto se úprava v mnohém jejich právní úpravou inspiruje, zejména pak při stanovení a výkladu požadavků vychází z etického kodexu auditora.*

Tento dokument slouží jako rozpracované teze budoucí vyhlášky a je proto podkladem k další diskuzi. Může se měnit a to v závislosti jak na obsahu připomínek odborné veřejnosti, tak na obsahu připomínek v průběhu legislativního procesu.

Návrh

VYHLÁŠKA

ze dne dd.mm.rrrr

o autorizovaných inspektorech

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § X zákona č. X, o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti):

ČÁST PRVNÍ
OBECNÁ

§ 1
Předmět úpravy

Tato vyhláška upravuje

a) požadavky pro udělení autorizace inspektora,
b) náležitosti a průběh odborné zkoušky žadatelů o autorizaci,
c) výkon činnosti inspektora,
d) podmínky na výkon činnosti inspektora.

ČÁST DRUHÁ
ZVLÁŠTNÍ

HLAVA I
POŽADAVKY PRO UDĚLENÍ AUTORIZACE INSPEKTORA

§ 2
Žádost fyzické osoby o udělení autorizace

1) Žádost fyzické osoby o udělení autorizace (dále jen „žádost o udělení autorizace“) obsahuje
   a) jméno nebo jména, pokud jich žadatel má více, příjmení a akademický titul žadatele, pokud jej žadatel získal a žádá o zápis tohoto titulu do seznamu inspektorů,
   b) adresu sídla, a pokud žadatel nemá sídlo, adresu místa trvalého pobytu nebo místa pobytu podle druhu pobytu cizince na území České republiky,

c) kontaktní adresu na území České republiky v případě, že žadatel nemá sídlo nebo místo trvalého pobytu podle druhu pobytu cizince na území České republiky,
d) identifikační číslo osoby, a pokud jej žadatel nemá, datum narození žadatele,
e) telefonní kontakt,
f) adresu elektronické pošty nebo adresu internetové stránky týkající se výkonu činnosti inspektora, pokud žadatel žádá o zápis této adresy do seznamu inspektorů,
g) jinou adresu pro doručování sdělenou žadatelem nebo údaj, že jinou adresou pro doručování je adresa elektronické pošty podle písmene f), pokud žadatel žádá o doručování na jinou adresu pro doručování, a
h) datum a podpis.

2) Žadatel připojí k žádosti o udělení autorizace doklady prokazující splnění požadavků pro udělení autorizace inspektora podle § X odst. 1 písm. b) až d) *[Inspektoři]* zákona.
3) Vzor žádosti je uveden v příloze č. 1 k této vyhlášce.

§ 3
Bezúhonnost

1) Podmínku bezúhonnosti nesplňuje osoba, která byla pravomocně odsouzena za jakýkoliv úmyslný trestný čin nebo trestný čin spáchaný z nedbalosti v souvislosti s výkonem činnosti inspektora nebo auditora, nehledí-li se na ni, jako by nebyla odsouzena.
2) Splnění podmínky bezúhonnosti se dokládá výpisem z evidence Rejstříku trestů ne starším než 3 měsíce.
3) Bezúhonnost se kromě výpisu z evidence Rejstříku trestů dokládá také
   a) u fyzické osoby, která se v posledních 3 letech zdržovala nepřetržitě po dobu delší než 3 měsíce v cizím státě, výpisem z evidence trestů nebo rovnocenným dokladem vydaným příslušným soudním nebo správním orgánem tohoto státu, nebo výpisem z evidence Rejstříku trestů, v jehož příloze jsou tyto informace obsaženy,
   b) u fyzické osoby, která není státním občanem České republiky, výpisem z evidence trestů nebo rovnocenným dokladem vydaným příslušným soudním nebo správním orgánem státu, jehož je tato osoba občanem, nebo výpisem z evidence Rejstříku trestů, v jehož příloze jsou tyto informace obsaženy.

§ 4
Odborná způsobilost

Za odborně způsobilou podle § X odst. 2 písm. d) *[Inspektoři]* zákona se považuje osoba, která splňuje požadavky na

a) dosažené vzdělání, délku praxe a další požadavky prokazující odbornou způsobilost podle § 5 této vyhlášky a

b) úspěšně složila zkoušku inspektora podle § 6 a § 7 této vyhlášky.

§ 5
Vzdělání a praxe

1) Žadatel o autorizaci musí být držitelem osvědčení nebo certifikace auditora nebo auditora kybernetické bezpečnosti podle technické normy[1] nebo srovnatelného mezinárodního certifikátu nebo osvědčení prokazujícího způsobilosti vykonávat audit kybernetické a informační bezpečnosti.
2) Žadatel o autorizaci musí dále splňovat alespoň jednu z následujících kombinací požadavků na vzdělání a praxi:
   a) úplné střední vzdělání nebo úplné střední odborné vzdělání a alespoň 10 let praxe v oblasti informačních technologií nebo kybernetické bezpečnosti nebo alespoň 7 let praxe v oblasti auditu informačních systémů;
   b) vysokoškolské vzdělání v bakalářském studijním programu a alespoň 7 let praxe v oblasti informačních technologií nebo kybernetické bezpečnosti nebo alespoň 5 let praxe v oblasti auditu informačních systémů;
   c) vysokoškolské vzdělání v magisterském studijním programu a alespoň 5 let praxe v oblasti informačních technologií nebo kybernetické bezpečnosti nebo alespoň 3 let praxe v oblasti auditu informačních systémů.
3) Splnění požadavku na vzdělání se prokazuje předložením dokladu o dosaženém vzdělání. Splnění požadavku na praxi se prokazuje předložením osvědčení o řádném výkonu činnosti s kontaktem na ověření reference nebo seznamu provedených auditů nebo kontrol osvědčujícího pravidelný výkon auditní činnosti v požadovaném období včetně kontaktu na ověření reference.

§ 6
Zkouška inspektora

1) Žadatel se na zkoušku hlásí prostřednictvím rezervačního systému na internetových stránkách Úřadu. Termíny pro vykonání zkoušky jsou zveřejňovány průběžně s dostatečným časovým předstihem včetně uvedení maximálního počtu žadatelů o zkoušku, formy zkoušky a místa jejího konání.
2) Poplatek za umožnění vykonání zkoušky činí 25.000 Kč. Poplatek je potřeba uhradit před vykonáním zkoušky. V opačném případě nebude žadatel k vykonání zkoušky připuštěn.
3) Úspěšně vykonaná zkouška má pro potřeby § X odst. 1 *[Inspektoři]* zákona platnost 1 rok ode dne vykonání.
4) Změnu termínu zkoušky je možné provést bezplatně nejpozději do 30 dnů před dnem vykonání zkoušky. Změna termínu zkoušky v kratším termínu je zpoplatněna

[1] Např. STN EN ISO/IEC řady 27000 nebo ISO řady 17000.

částkou 15.000 Kč. Změnu termínu zkoušky lze provést nejpozději 7 dnů před dnem vykonání zkoušky.

5) V případě nedostavení se k rezervovanému termínu se zkouška považuje za nesloženou a zaplacený poplatek za vykonání zkoušky nebo změnu termínu zkoušky propadá bez náhrady. Z důvodů hodných zvláštního zřetele může Úřad propadnutí poplatku prominout.
6) V případě, že termín zkoušky zruší Úřad, nabídne přihlášeným žadatelům náhradní termín, nebo zaplacený poplatek vrátí.

§ 7
Forma a průběh zkoušky inspektora

1) Odborná zkouška inspektora kybernetické bezpečnosti se provádí formou písemného testu ze znalostí obecně závazných právních předpisů upravujících kybernetickou bezpečnost a postupy při kontrole. Zkouška ověřuje splnění minimálních požadavků na znalosti, schopnosti a předpoklady a odbornou způsobilost inspektora pro proces kontroly uvedené v příloze č. 3 k této vyhlášce. Zkouška se koná v českém jazyce.
2) Zkušební otázky mají podobu vědomostní otázky nebo příkladu s jednoznačným zadáním úkolu a čtyř alternativních možností odpovědí, z nichž je vždy pouze jedna správná. Každá otázka je bodově ohodnocena. Ve výsledné sadě je vygenerováno 100 zkušebních otázek, tak aby byly zastoupeny všechny zkušební okruhy. Časový rozsah zkoušky je 150 minut.
3) Úřad na svých internetových stránkách zveřejňuje okruhy a příklady otázek k provedení odborné zkoušky, pokyny pro jejich používání, pokyny pro průběh zkoušky a vzor žádosti o provedení zkoušky.
4) Test může být zadán fyzicky v předem určených prostorách, nebo elektronicky pomocí vhodných technických prostředků.
5) Před zahájením odborné zkoušky žadatel prokáže svou totožnost průkazem totožnosti a pověřený zaměstnanec Úřadu jej poučí o pravidlech pro provádění zkoušky. Pokud uchazeč nepředloží průkaz totožnosti před zahájením zkoušky nebo se při zkoušce chová v rozporu s pravidly upravujícími průběh zkoušky nebo dobrými mravy, je ze zkoušky vyloučen a má se za to, že u zkoušky neuspěl. Odborná zkouška prováděná elektronicky musí být po celou dobu přípravy a provádění zkoušky monitorována pomocí videokonferenčních nástrojů a nástrojů pro vzdálený přístup.
6) Zkouška se považuje za úspěšně složenou, pokud uchazeč dosáhne alespoň 80 % správných odpovědí.
7) Za vyhodnocení testu odpovídá pověřený zaměstnanec Úřadu nebo jiná pověřená osoba. Výsledek testu je uchazeči sdělen do 15 pracovních dnů ode dne vykonání testu.

HLAVA II
VÝKON ČINNOSTI INSPEKTORA

§ 8
Výběr inspektora Úřadem

Úřad se při výběru inspektora podle § X odst. 3 *[Kontrola vykonávaná inspektory]* zákona řídí vzestupně řazeným abecedním seznamem příjmení inspektorů. Úřad při výběru inspektora zohlední specifické okolnosti případu. Pokud ustanovený inspektor nebude schopen z vážných důvodů kontrolu vykonat, Úřad ustanoví dalšího inspektora v pořadí.

§ 9
Určení délky trvání kontroly

1) Před zahájením kontroly inspektor určí přiměřenou dobu trvání kontroly, aby bylo možné provést řádnou kontrolu v určeném rozsahu zajištění minimální úrovně kybernetické bezpečnosti podle prováděcího právního předpisu. *[Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu nižších povinností]*.
2) Výpočet kontrolních dnů se provádí pro celkové prostředí poskytovatele regulované služby v následujícím pořadí
   a) výpočet základního počtu dnů kontroly,
   b) uplatnění dalších faktorů ovlivňujících délku trvání kontroly.,
3) Při výpočtu doby trvání kontroly se zohlední zejména:
   a) velikost organizace,
   b) počet lokalit organizace a jejich geografické rozmístění,
   c) stanovený rozsah podle § X *[Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby]* zákona,
   d) množství, komplexnost bezpečnostních politik a bezpečnostní dokumentace,
   e) počet interních a externích smluvních pracovníků zapojených do provozu regulované služby,
   f) zkušenosti inspektora s daným odvětvím.
4) Výpočet základní doby trvání kontroly se provede na základě počtu interních a externích zaměstnanců, kteří se podílejí na provozu regulované služby, tabulka pro určení doby trvání kontroly je uvedena v příloze č. 2 této vyhlášky.

§ 10
Harmonogram kontroly

1) Inspektor vypracuje před zahájením kontroly harmonogram kontroly, který zahrnuje povahu, časový průběh a rozsah kontrolních postupů, které mají být provedeny za účelem získání dostatečných podkladů kontrolních zjištění.

Harmonogram kontroly slouží jako záznam správného naplánování a provedení kontrolních postupů.

2) Harmonogram kontroly je přílohou protokolu o kontrole.

HLAVA III
PODMÍNKY VÝKONU ČINNOSTI INSPEKTORA

§ 11
Etický kodex inspektora

1) Etický kodex inspektora definuje základní etické principy, které inspektor aplikuje při výkonu své činnosti. Základními principy jsou integrita, nestrannost, odborná způsobilost a řádná péče, mlčenlivost a profesionální jednání.
2) Inspektor identifikuje hrozby ohrožující dodržování základních principů, hodnotí je a v případě potřeby ošetřuje.

§ 12
Integrita

Inspektor jedná ve všech profesních a obchodních vztazích poctivě a čestně.

§ 13
Nestrannost

Inspektor uplatňuje odborný úsudek a neohrozí jej předpojatostí, střetem zájmů nebo nepatřičným vlivem jiných fyzických osob, organizací nebo technologií či jiných faktorů nebo kvůli nepatřičnému spoléhání na jiné fyzické osoby, organizace nebo technologie.

§ 14
Odborná způsobilost a řádná péče

1) Inspektor si osvojuje a udržuje odborné znalosti a dovednosti na takové úrovni, aby služby, které poskytuje, byly provedeny na odborné úrovni a odpovídaly současným profesním standardům a příslušné legislativě.
2) Inspektor jedná svědomitě a v souladu s příslušnými odbornými a profesními standardy.

§ 15
Mlčenlivost

Inspektor zachovává důvěrný charakter informací získaných v rámci profesních a obchodních vztahů.

§ 16
Profesionální jednání

Inspektor dodržuje příslušné právní předpisy, chová se při výkonu veškerých odborných činností a ve všech obchodních vztazích v souladu s profesní povinností jednat ve veřejném zájmu a vyhýbá se každému jednání, o němž ví nebo by měl vědět, že by mohlo diskreditovat jeho profesi.

§ 17
Odpovědnost inspektora

1) Inspektor odpovídá za správnost, rozsah a odbornost při provádění kontroly zavedení a provádění bezpečnostních opatření a za vypracování protokolu o kontrole.
2) Inspektor provádí kontrolu profesionálně, objektivně, nestranně a nezávisle na základě důkazů.

ČÁST TŘETÍ
ÚČINNOST

§ 18
Účinnost

Tato vyhláška nabývá účinnosti dnem dd.mm.rrrr.

Ředitel:
Ing. Lukáš Kintr v. r.

Příloha č. 1 k vyhlášce č. XX/XXXX Sb.
Vzor žádosti o udělení autorizace

ŽÁDOST

o udělení - opakované udělení[2]

autorizace podle § X odst. 1 *[Inspektoři]* zákona o kybernetické bezpečnosti

Jméno, případně jména, příjmení, případně akademický titul, pokud má být zapsán do seznamu autorizovaných inspektorů:
Adresa sídla, místa trvalého pobytu nebo místa pobytu podle druhu pobytu cizince na území České republiky:
Kontaktní adresa na území České republiky, nemá-li žadatel sídlo nebo místo trvalého pobytu podle druhu pobytu cizince na území České republiky:
Identifikační číslo osoby/datum narození žadatele:
Telefonní kontakt žadatele:

2 Nehodící se škrtněte.

Adresa elektronické pošty nebo internetové stránky týkající se výkonu činnosti inspektora, pokud žadatel žádá o zápis adresy do seznamu autorizovaných inspektorů jako veřejného údaje:
Jiná adresa pro doručování nebo údaj, že jinou adresou pro doručování je výše uvedená adresa elektronické pošty, žádá-li žadatel o doručování na jinou adresu pro doručování:
Datum a podpis:

Přílohy k žádosti:[3]

3 Vyplní žadatel.

Příloha č. k vyhlášce č. XX/XXXX Sb.
Tabulka pro výpočet doby trvání kontroly

Celkový počet zaměstnanců podílejících se na provozu regulované služby	Základní rozsah kontroly v člověkodnech
1~10	5
11~20	6
21~30	7
31~40	8
41~50	9
51~60	10
>60	+ jeden den za každých dalších 20 zaměstnanců
Není třeba zvyšovat počet kontrolních dnů, pokud jsou přítomni zaměstnanci z jiných pracovišť nebo se podílejí na provozu regulované služby prostřednictvím vzdáleného připojení.	

Doba trvání kontroly uvedená v této tabulce je určena ve vztahu k dnům inspektora, strávených při kontrole. Základem výpočtu je 8 hodinový pracovní den. Cena za jednu auditohodinu je stanovena na 1350 Kč.

Příloha č. 3 k vyhlášce XX/XXXX Sb.
Minimální požadavky na odbornou způsobilost inspektora

1. Znalost procesů a systémů řízení kybernetické a informační bezpečnosti.
2. Znalost zásad organizace kybernetické a informační bezpečnosti.
3. Znalost zásad personální bezpečnosti.
4. Znalost zásad řízení přístupů.
5. Znalost o způsobu používání kryptografických bezpečnostních mechanismů.
6. Znalost principů testování kybernetické bezpečnosti.
7. Znalost zásad auditu kybernetické bezpečnosti a principů a procesů provádění auditů.
8. Znalost obecně závazných právních předpisů regulujících kybernetickou bezpečnost a relevantních mezinárodních norem.
9. Znalost obecně závazných právních předpisů regulujících ochranu osobních údajů.
10. Znalost standardů a zásad z oblasti ochrany osobních údajů.
11. Schopnost navrhovat a uplatňovat bezpečnostní strategie a politiky.
12. Znalost procesů a metod řízení rizik.
13. Znalost postupů hodnocení rizik.
14. Znalost typických kybernetických hrozeb a postupů pro identifikaci hrozeb a zranitelností.
15. Znalost bezpečnostních mechanismů.
16. Znalost metodik architektury kybernetické bezpečnosti.
17. Znalost procesů řešení kybernetických bezpečnostních incidentů.
18. Znalost principů havarijního plánování a plánů obnovy.
19. Znalost procesů řízení kontinuity činností.
20. Znalost principů logování a bezpečnostního monitoringu.
21. Znalost zásad řízení a bezpečnostních mechanismů fyzické bezpečnosti.
22. Znalost principů řízení služeb v oblasti informačních technologií.
23. Znalost principů řízení nákladů a rozpočtových pravidel.
24. Schopnost prioritizace úkolů a efektivního přiřazování zdrojů.
25. Znalost principů řízení lidských zdrojů.
26. Znalost konceptů počítačových sítí.
27. Znalost zásad řízení projektů.
28. Znalost zásad řízení dodavatelských služeb a bezpečnosti dodavatelského řetězce.
29. Znalost zásad vývoje aplikací a informačních systémů.
30. Znalost zásad provozování informačních systémů.
31. Znalost zásad aplikační bezpečnosti.
32. Technické vědomosti o auditovaných systémech.
33. Znalost metod posuzování rizik v míře nezbytné pro vyhodnocení rizik auditu a posouzení hodnocení rizik.
34. Schopnost posoudit důkazy.
35. Schopnost analyzovat rizika.
36. Schopnost zpracovat úplnou a přehlednou závěrečnou zprávu o výsledcích auditu.
37. Schopnost analyzovat a hodnotit bezpečnostní mechanismy a řešení.