122

VYHLÁŠKA
ze dne 25. června 2026

o plánu odolnosti, posouzení rizik, opatřeních k zajištění odolnosti subjektů kritické infrastruktury a o hlášení incidentu

Ministerstvo vnitra stanoví podle § 29 odst. 2 zákona č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře) k provedení § 14 odst. 6, § 15 odst. 2 a § 19 odst. 5 zákona o kritické infrastruktuře:

ČÁST PRVNÍ
ÚVODNÍ USTANOVENÍ

§ 1
Předmět úpravy

Tato vyhláška upravuje

a) náležitosti a způsob zpracování plánu odolnosti a posouzení rizik subjektu kritické infrastruktury,
b) obsah technických, bezpečnostních a organizačních opatření k zajištění odolnosti subjektu kritické infrastruktury (dále jen „opatření k zajištění odolnosti“) a
c) parametry incidentu, podrobnosti rozsahu hlášených informací a způsob předávání informací o incidentu.

§ 2
Vymezení pojmů

Pro účely této vyhlášky se rozumí

a) technickými opatřeními soubor technických, technologických, stavebních, informačních nebo provozních prostředků, systémů a řešení, včetně jejich architektury a konfigurace, které subjekt kritické infrastruktury zavádí při zajišťování jeho odolnosti a při řešení incidentů zejména za účelem prevence, predikce, detekce a reakce na incidenty a za účelem jejich zvládnutí nebo omezení jejich dopadů,
b) organizačními opatřeními soubor pravidel, procesů, postupů, odpovědností a způsobů řízení, včetně plánovacích, koordinačních, kontrolních a rozhodovacích mechanismů, které upravují

činnost subjektu kritické infrastruktury při zajišťování jeho odolnosti a při řešení incidentů zejména za účelem prevence, predikce, detekce a reakce na incidenty a za účelem jejich zvládnutí nebo omezení jejich dopadů,

c) bezpečnostními opatřeními opatření personálního, režimového, kontrolního nebo ochranného charakteru, která jsou zaměřena na ochranu osob, majetku, informací, procesů nebo činností subjektu kritické infrastruktury před úmyslným protiprávním jednáním, při zajišťování jeho odolnosti a při řešení incidentů zejména za účelem prevence, predikce, detekce a reakce na incidenty a za účelem jejich zvládnutí nebo omezení jejich dopadů, pokud nejde o technická nebo organizační opatření,

d) fyzickou bezpečností soubor opatření fyzické ochrany zaměřený zejména na ochranu majetku, osob a kritické infrastruktury před neoprávněným přístupem, poškozením, odcizením, neoprávněným zásahem nebo zničením,

e) objektem budova nebo areál budov, stavba, technologické zařízení, komunikace, infrastruktura, pozemek nebo vnitřní prostor v budově,

f) bezpečnostním perimetrem souvisle vymezená oblast v okolí kritické infrastruktury stanovující chráněnou zónu, která obepíná objekt, ve kterém se nachází kritická infrastruktura, a jeho bezprostředně přiléhající pozemky a prostor nad tímto objektem, v rozsahu nezbytném k zajištění jeho ochrany, a

g) nežádoucí událostí událost, která může narušit poskytování základní služby nebo jinou činnost subjektu kritické infrastruktury související s poskytováním základní služby a po jejímž vyhodnocení může být klasifikována jako incident.

ČÁST DRUHÁ

POSOUZENÍ RIZIK SUBJEKTU KRITICKÉ INFRASTRUKTURY A PLÁN ODOLNOSTI

§ 3

Posouzení rizik

(1) Subjekt kritické infrastruktury zpracuje posouzení rizik subjektu kritické infrastruktury v rámci dokumentace posouzení rizik. Zpracování dokumentace posouzení rizik v souladu s ČSN ISO 31000 se považuje za zpracování v souladu s požadavky této vyhlášky.

(2) Dokumentace posouzení rizik obsahuje

a) základní informace v rozsahu

1. identifikace rizika,
2. analýzy rizika,
3. hodnocení rizika a
4. popisu postupu při ošetření rizika,

b) popis techniky posuzování rizik a její aplikace a

c) posouzení rizik zohledňující skutečnosti podle písmene a) a podle odstavce 1.

(3) Subjekt kritické infrastruktury použije techniku posuzování rizik podle přílohy B ČSN EN IEC 31010 nebo jinou techniku umožňující dosažení srovnatelné míry systematičnosti a průkaznosti výsledků jako užití techniky podle této normy.

(4) Při identifikaci rizik vychází subjekt kritické infrastruktury z posouzení rizik České republiky v návaznosti na nepřijatelná rizika v jednotlivých odvětvích a pododvětvích a z hrozeb specifických pro jím poskytovanou základní službu.

(5) Analýza rizik obsahuje rozbor povahy rizika a jeho vlastností. V rámci analýzy rizik se posuzuje
   a) povaha a typ nejistoty související s rizikem,
   b) zdroj možného rizika,
   c) předpokládaný následek související s rizikem,
   d) pravděpodobnost výskytu rizika v souvislosti s incidentem a
   e) postupy a opatření pro zvládání rizik.

(6) Při analýze rizik stanoví subjekt kritické infrastruktury
   a) pravděpodobnost vzniku hrozby podle tabulky č. 1 v příloze č. 1 k této vyhlášce a
   b) dopady hrozby na jím poskytovanou základní službu podle tabulky č. 2 v příloze č. 1 k této vyhlášce.

(7) Součinem hodnot pravděpodobnosti a dopadu hrozby podle odstavce 6 subjekt kritické infrastruktury vypočítá úroveň rizika.

(8) Hodnocení rizik obsahuje porovnání výsledků analýzy rizik s předem stanovenými kritérii přijatelnosti rizik. V rámci hodnocení rizik subjekt kritické infrastruktury s ohledem na vypočítaná rizika stanoví jejich úroveň podle tabulky č. 3 v příloze č. 1 k této vyhlášce. Na základě stanovení úrovně rizik a s ohledem na zavedená opatření stanoví subjekt kritické infrastruktury přijatelná, podmínečně přijatelná a nepřijatelná rizika.

(9) V rámci popisu postupu při ošetření rizika subjekt kritické infrastruktury popíše postup výběru a realizace opatření k řízení nepřijatelného rizika a podmínečně přijatelného rizika.

(10) Subjekt kritické infrastruktury při zpracování posouzení rizik subjektu kritické infrastruktury vyhodnotí veškerá rizika související s činností člověka, přírodními vlivy, technickými selháními a haváriemi, která by mohla vést k incidentu. Dále vyhodnotí rizika týkající se jeho závislosti na jiných poskytovaných základních službách, hrozby přeshraniční povahy, mimořádné události v oblasti veřejného zdraví, hybridních nebo jiných podobných hrozeb, ozbrojeného konvenčního konfliktu a teroristických útoků.

(11) Při analýze a hodnocení rizik lze využít jiného postupu než podle přílohy č. 1 k této vyhlášce, pokud se tímto postupem dosáhne alespoň srovnatelného výsledku, kterého by bylo dosaženo postupem podle přílohy č. 1 k této vyhlášce.

Náležitosti a způsob zpracování plánu odolnosti

§ 4

(1) Úvodní strana plánu odolnosti obsahuje
   a) nadpis „Plán odolnosti“,

b) název subjektu kritické infrastruktury,
c) datum zpracování plánu odolnosti,
d) jméno a podpis zpracovatele,
e) datum schválení a
f) jméno a podpis schvalovatele.

(2) Plán odolnosti musí být zpracován v elektronické a listinné podobě v českém jazyce.

(3) Plán odolnosti se ukládá takovým způsobem, aby byl dostupný zaměstnancům v rozsahu odpovídajícím jejich pracovnímu zařazení a povinnostem k zabezpečení základní služby.

§ 5

(1) Plán odolnosti se skládá z informační, operativní a pomocné části.

(2) Informační část obsahuje
a) základní informace o subjektu kritické infrastruktury a popis případné vazby na další subjekty kritické infrastruktury v rámci koncernu,
b) popis poskytovaných základních služeb a informaci, zda je pro danou základní službu subjekt kritické infrastruktury subjektem evropské kritické infrastruktury,
c) popis postupu, který byl využit pro identifikaci kritické infrastruktury,
d) přehled kritické infrastruktury subjektu kritické infrastruktury,
e) popis postupu pro určení vazeb mezi funkčními celky kritické infrastruktury subjektu kritické infrastruktury, při které subjekt kritické infrastruktury posoudí existenci přímého nebo nepřímého vlivu vazby, možnost nahrazení vazby a časovou charakteristiku vazby,
f) přehled vazeb mezi funkčními celky kritické infrastruktury subjektu kritické infrastruktury,
g) seznam kritických pracovníků,
h) popis zdrojů nezbytných k zajištění poskytování základní služby a informací o způsobu zabezpečení nezbytných věcných prostředků a
i) přehled kritických dodavatelů.

(3) Operativní část obsahuje
a) přehled nepřijatelných rizik a podmínečně přijatelných rizik,
b) přehled závislosti jednotlivých odvětví, pododvětví a základních služeb na základní službě poskytované subjektem kritické infrastruktury,
c) přehled opatření k zajištění odolnosti v souladu s částí třetí v rozsahu

1. popisu cíle a přínosu opatření,
2. předpokládaných lidských, finančních a technických zdrojů pro zavedení opatření,
3. termínu a způsobu zavedení opatření a
4. popisu vazeb mezi riziky a opatřeními a

d) plán komunikace a přehled spojení se subjekty podílejícími se na zajišťování základní služby a na řešení incidentů.

(4) Pomocná část obsahuje
a) zásady manipulace s plánem odolnosti,

b) přehled právních předpisů a technických norem využitých při přijímání opatření k zajištění odolnosti subjektu kritické infrastruktury,

c) odkaz na dokumentaci posouzení rizik,

d) přehled geografických podkladů a

e) seznam dokumentů souvisejících s přijímáním opatření k zajištění odolnosti subjektu kritické infrastruktury.

ČÁST TŘETÍ

OPATŘENÍ K ZAJIŠTĚNÍ ODOLNOSTI SUBJEKTU KRITICKÉ INFRASTRUKTURY

§ 6

Řízení rizik

(1) Subjekt kritické infrastruktury za účelem realizace ošetření rizik na základě výsledků provedeného hodnocení rizik zavádí systém řízení rizik a provádí opatření pro zvládání nepřijatelných rizik a podmínečně přijatelných rizik, a to při zohlednění postupů a zásad daných ČSN ISO 31000 nebo jiných postupů, které povedou k dosažení účelu odpovídajícího postupům a zásadám podle této normy.

(2) Subjekt kritické infrastruktury může v rámci řízení rizik na základě výsledků posouzení rizik subjektu kritické infrastruktury s ohledem na odolnost vůči identifikovaným rizikům stanovit rozsah jednotlivých opatření k zajištění odolnosti, popřípadě za jakých podmínek je možno vyloučit jejich přijetí.

§ 7

Zajištění kontinuity činností

(1) Subjekt kritické infrastruktury při přijímání opatření k zajišťování kontinuity činností vychází z postupů a zásad stanovených v ČSN EN ISO 22301.

(2) Subjekt kritické infrastruktury pro zajištění kontinuity činností v rámci opatření zajišťujícího jeho odolnost vypracuje metodiku, která obsahuje postup pro provedení analýzy dopadů, a zpracuje plán zajištění kontinuity činností, v rámci kterého

a) provádí analýzu dopadů, která obsahuje vyhodnocení možných dopadů na poskytování základní služby,

b) zohlední výsledky posouzení rizik subjektu kritické infrastruktury,

c) stanoví na základě výstupů analýzy dopadů cíle zajištění kontinuity činností formou určení

1. minimální úrovně požadavků, která je nezbytná pro poskytování základní služby, a
2. doby, během které je možné po incidentu obnovit minimální úroveň poskytované základní služby,

d) stanoví postup pro naplnění cílů podle písmene c).

(3) Subjekt kritické infrastruktury plán zajištění kontinuity činností minimálně jednou za 4 roky testuje a v návaznosti na zjištěné poznatky aktualizuje. Testování plánu zajištění kontinuity činností probíhá zejména formou penetračních nebo zátěžových testů.

§ 8

Příprava a odezva na incidenty

(1) Subjekt kritické infrastruktury v rámci opatření k přípravě a odezvě na incidenty

a) zpracuje vnitřní nastavení procesů a pravidel, v rámci kterého stanoví

1. nástroje a prostředky pro identifikaci, zaznamenání a vyhodnocení incidentu,
2. postup pro identifikaci, zaznamenání a vyhodnocení incidentu,
3. způsob komunikace při koordinaci řešení incidentu a jeho zvládání, včetně k tomu určených prostředků, a
4. odpovědnost pracovníků za identifikaci, zaznamenání a vyhodnocení incidentu a za koordinaci řešení incidentu a jeho zvládání,

b) určí nástroje a postupy pro sběr, získání a uchování informací potřebných pro zpracování hlášení o incidentu a

c) zpracuje postup pro opatření k zajištění odolnosti pro koordinaci řešení incidentu a jeho zvládání.

(2) Subjekt kritické infrastruktury v rámci opatření k odezvě na incidenty dále

a) prošetří příčiny incidentu,

b) vede záznamy o incidentech a o jejich zvládání a

c) vyhodnotí účinnost řešení incidentu a stanoví, popřípadě aktualizuje stávající nutná opatření k zajištění odolnosti pro zamezení opakování incidentu.

(3) Záznam o incidentu a o jeho zvládání obsahuje

a) datum a čas vzniku incidentu, jsou-li tyto údaje známy,

b) datum a čas identifikace incidentu,

c) dobu trvání incidentu,

d) povahu incidentu,

e) příčinu incidentu, je-li známa,

f) důsledky incidentu,

g) informaci o případném přeshraničním dopadu incidentu,

h) odhadovaný počet uživatelů, kteří byli incidentem ovlivněni, a jejich podíl v rámci dané základní služby,

i) dobu, po kterou bylo narušeno poskytování základní služby,

j) způsob, jakým byl incident zvládnut,

k) návrh pro snížení rizika opakovaného vzniku incidentu a

l) výčet ostatních základních služeb, jejichž poskytování bylo vlivem incidentu narušeno.

§ 9

Fyzická bezpečnost

(1) Subjekt kritické infrastruktury v rámci opatření souvisejícího s fyzickou bezpečností předchází narušení kritické infrastruktury, neoprávněným zásahům do ní a narušení poskytování základní služby. Za tímto účelem, je-li to technicky možné nebo účelné,

a) stanoví bezpečnostní perimetr,

b) může s ohledem na umístění kritické infrastruktury rozdělit bezpečnostní perimetr do jednotlivých zón s odlišnou úrovní fyzické ochrany,

c) stanoví u každé zóny podle písmene b) s ohledem na její úroveň fyzické ochrany opatření a

d) stanoví systém fyzické ochrany

1. k zamezení neoprávněnému vstupu,
2. k zamezení poškození, odcizení nebo zneužití kritické infrastruktury, neoprávněného zásahu do kritické infrastruktury a narušení poskytování základní služby,
3. k ochraně budov a jiných určených prostor a
4. k evidenci vstupů a přístupů do bezpečnostního perimetru.

(2) Subjekt kritické infrastruktury v souladu s výsledky posouzení rizik subjektu kritické infrastruktury vyhodnotí potřebu zavedení opatření.

(3) Mezi prostředky technických opatření patří, je-li to technicky možné nebo účelné, zejména

a) mechanické zábranné prostředky,

b) poplachový zabezpečovací a tísňový systém,

c) dohledové videosystémy,

d) systémy kontroly a evidence vstupu,

e) systémy přivolání pomoci,

f) poplachové přenosové systémy a zařízení,

g) kombinované a integrované systémy,

h) přístroje pro použití ve dveřních vstupních audiosystémech a videosystémech,

i) dohledová a poplachová přijímací centra,

j) nouzové zvukové systémy a hlasová výstražná zařízení,

k) bezpečnostní bezpilotní systémy k monitoringu chráněných prostor, detekční systémy ke zjištění přítomností cizích bezpilotních systémů, nebo

l) detekční technologie ke zjištění přítomnosti cizích osob nebo zařízení.

(4) U souboru obdobných objektů může subjekt kritické infrastruktury stanovit opatření typově podle kategorií objektů a rizikové úrovně, pokud je zajištěna přiměřenost a prokazatelnost opatření podle odstavce 1.

§ 10

Řízení bezpečnosti pracovníků

(1) Subjekt kritické infrastruktury v rámci opatření k zajištění své odolnosti ve vztahu k pracovníkům

a) identifikuje a určuje své kritické pracovníky,

b) zpracovává opatření pro snížení rizik spojených s kritickými pracovníky na základě výsledků posouzení rizik subjektu kritické infrastruktury a

c) informuje v nezbytně nutném rozsahu kritického pracovníka o přijatých opatřeních podle písmene b).

(2) Subjekt kritické infrastruktury v rámci opatření podle odstavce 1

a) vytvoří postup pro identifikaci a určování kritických pracovníků v rozsahu stanovení

1. pozic, popřípadě kategorií pracovníků s ohledem na vykonávané funkce nezbytné pro poskytování základní služby,
2. přístupových práv k informacím citlivé povahy, ke kritické infrastruktuře, popřípadě do jednotlivých zón oblasti vymezené bezpečnostním perimetrem, a
3. požadavku na odbornou přípravu a kvalifikaci,

b) vytvoří postup pro ověřování spolehlivosti pracovníků stanovením

1. pozic, popřípadě kategorií pracovníků, u kterých je ověřována spolehlivost,
2. způsobu a četnosti kontroly dokumentů k prokázání totožnosti a bezúhonnosti a
3. osoby provádějící kontrolu podle bodu 2,

c) stanoví činnosti manažera kritické infrastruktury v rámci subjektu kritické infrastruktury a

d) zpracuje plán rozvoje bezpečnostního povědomí, který obsahuje

1. způsob poučení jím určeného vrcholného vedení o jeho povinnostech v systému řízení rizik a řízení kontinuity činností a
2. způsob poučení pracovníků a kritických pracovníků o jejich povinnostech a školení pracovníků v oblasti ochrany kritické infrastruktury subjektu kritické infrastruktury.

(3) Subjekt kritické infrastruktury dále v rámci opatření souvisejících s řízením bezpečnosti pracovníků

a) určí osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu rozvoje bezpečnostního povědomí uvedeny, a

b) zpracuje plán kontrolní činnosti pro dodržování stanovených opatření k zajištění odolnosti ze strany pracovníků a kritických pracovníků.

(4) Subjekt kritické infrastruktury vede o poučení a školení podle odstavce 2 písm. d) přehledy obsahující datum, předmět poučení a školení a seznam osob, které poučení a školení absolvovaly.

§ 11

Řízení bezpečnosti dodavatelského řetězce

(1) Subjekt kritické infrastruktury v rámci opatření k zajištění své odolnosti ve vztahu k dodavateli

a) zpracovává opatření pro snížení rizik spojených s kritickými dodavateli nebo dodavatelskými řetězci na základě výsledků posouzení rizik subjektu kritické infrastruktury,

b) informuje v nezbytně nutném rozsahu dodavatele nebo kritického dodavatele o přijatých opatřeních souvisejících s dodavatelem, dodavatelským řetězcem nebo kritickým dodavatelem a

c) eviduje své kritické dodavatele.

(2) Informace o přijatých opatřeních souvisejících s kritickým dodavatelem obsahuje údaj o
   a) zařazení subjektu na seznam subjektů kritické infrastruktury,
   b) poskytované základní službě,
   c) důvodech označení dodavatele za kritického dodavatele a
   d) způsobu zajištění mlčenlivosti kritického dodavatele o informacích uvedených v písmenech a) až c).

ČÁST ČTVRTÁ
IDENTIFIKACE A HLÁŠENÍ INCIDENTU

§ 12
Parametry incidentu

(1) Subjekt kritické infrastruktury za účelem identifikace incidentu vyhodnotí rizika pro jeho základní službu v rámci posouzení rizik a identifikuje dopady nepřijatelných rizik. Na základě vyhodnocení rizik předběžně stanoví podle § 13 a příloh č. 2 a 3 k této vyhlášce možný rozsah dopadů významného narušení poskytování základní služby.

(2) V případě vzniku nežádoucí události subjekt kritické infrastruktury posoudí za účelem identifikace incidentu parametry této události v rámci jejích dopadů podle přílohy č. 3 k této vyhlášce. Při posouzení nežádoucí události vychází z možného rozsahu dopadů podle odstavce 1.

(3) Při stanovení rozsahu dopadů nežádoucí události subjekt kritické infrastruktury dále zohlední
   a) počet zasažených osob,
   b) velikost zasaženého území,
   c) délku trvání,
   d) ekonomické dopady,
   e) dopady na životní prostředí,
   f) závislost jiných základních služeb a
   g) dopad na poskytování základní služby v jiném členském státě Evropské unie.

(4) Subjekt kritické infrastruktury může použít při výpočtu úrovně významnosti dopadů nežádoucí události postup odlišný od postupu podle odstavců 1 až 3, pokud se jedná o postup funkčně rovnocenný.

§ 13
Výpočet úrovně významnosti dopadů nežádoucí události

(1) Subjekt kritické infrastruktury vypočítá úroveň významnosti dopadů nežádoucí události podle bodových hodnot podle přílohy č. 3 k této vyhlášce stanovených parametrů nežádoucí události v rámci jednotlivých kritérií A až G uvedených v příloze č. 2 k této vyhlášce.

(2) Subjekt kritické infrastruktury stanoví procentuální odhad úrovně významnosti dopadů nežádoucí události podle funkce

$$UVD = 100 \sum_{i=1}^{n} \frac{K_i V_i}{K_{i\,\max}},$$

kde *UVD* je úroveň významnosti dopadů [%]; K_i je bodová hodnota i-tého kritéria podle přílohy č. 3 k této vyhlášce; n je počet kritérií; V_i je hodnota váhy i-tého kritéria podle přílohy č. 3 k této vyhlášce; $K_{i\,max}$ je maximální hodnota i-tého kritéria podle přílohy č. 3 k této vyhlášce.

(3) V případě naplnění prahové hodnoty 35 % úrovně významnosti dopadů nežádoucí události je nežádoucí událost považována za incident a parametry takové nežádoucí události za parametry incidentu.

§ 14

Hlášení incidentu

(1) Způsobem předávání informací o incidentu je jejich předání prostřednictvím formuláře pro hlášení incidentu.

(2) Formulář pro hlášení incidentu nebo pro předání informací subjektem kritické infrastruktury obsahuje

a) nadpis

1. „Hlášení incidentu“,
2. „Prvotní hlášení incidentu“,
3. „Zpráva o pokroku“, nebo
4. „Závěrečná zpráva“,

b) jméno kontaktní osoby a kontaktní údaje a

c) identifikační údaje subjektu kritické infrastruktury a informace o poskytované základní službě, která byla zasažena incidentem.

(3) Hlášení incidentu obsahuje

a) informace o incidentu v rozsahu

1. popisu,
2. data a času zjištění,
3. místa vzniku,
4. příčiny vzniku,
5. shrnutí řešení incidentu, včetně jeho časové posloupnosti, a
6. popisu účinnosti souvisejících přijatých opatření,

b) informace vymezující dopad incidentu, v rozsahu

1. počtu uživatelů, kteří byli nebo jsou incidentem ovlivněni, a jejich podíl v rámci dané základní služby,
2. doby trvání narušení poskytování základní služby a doby působení incidentu, vyjádřené počtem minut, hodin, dnů, týdnů nebo měsíců,

3. slovního popisu rozlohy území zasaženého narušením poskytování základní služby,
4. dopadu incidentu na poskytování základní služby v jiném členském státě Evropské unie nebo do takového státu a
5. dopadu na jiného poskytovatele základní služby, pokud je takovýto dopad znám.

(4) Prvotní hlášení incidentu obsahuje informace podle odstavce 3 v rozsahu jejich dostupnosti.

(5) Zpráva o pokroku obsahuje

a) dostupné informace o nových skutečnostech týkajících se incidentu v rozsahu informací podle odstavce 3, které nebyly dostupné v rámci prvotního hlášení,

b) předpokládaný čas nutný pro vyřešení incidentu a pro obnovu poskytování základní služby,

c) vysvětlení, z jakého důvodu incident stále trvá, a

d) popis konkrétních činností, které byly učiněny pro řešení incidentu.

(6) Závěrečná zpráva obsahuje informace podle odstavce 3, které nebyly dostupné v rámci prvotního hlášení incidentu nebo zprávy o pokroku.

ČÁST PÁTÁ

ÚČINNOST

§ 15

Tato vyhláška nabývá účinnosti dnem 1. srpna 2026.

Ministr:

Mgr. Metnar v. r.

Příloha č. 1

Analýza a hodnocení rizik

1. Pro výpočet rizika a stanovení jeho úrovně podle tabulky č. 3, která definuje přijatelnost rizika, se použije výpočet podle funkce Riziko = Pravděpodobnost hrozby × Dopady. Pro výpočet se použije bodová hodnota odpovídající úrovně obou proměnných z tabulky č. 1 a tabulky č. 2.
2. Výsledná úroveň rizika značí přijatelnost nebo nepřijatelnost rizika, od čehož se odvíjí potřeba přijmout definovaná opatření.
3. **Tabulka č. 1: Stupnice pro hodnocení pravděpodobností**

Úroveň	Hodnota	Popis
Zanedbatelná	1	Hrozba neexistuje nebo je velmi nepravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 20 let.
Malá	2	Hrozba je málo pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 10 do 20 let.
Střední	3	Hrozba je pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 5 do 10 let.
Vysoká	4	Hrozba je velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Velmi vysoká	5	Hrozba je téměř jistá. Předpokládaná realizace hrozby je častější než jednou za rok.

4. **Tabulka č. 2: Stupnice pro hodnocení dopadů**

Úroveň	Hodnota	Popis
Zanedbatelná	1	Dopady nejsou žádné nebo pouze zanedbatelné. Poskytování základní služby není ovlivněno.
Malá	2	Dopady jsou rozpoznatelné. Poskytování základní služby je částečně ovlivněno, ale nedochází k výraznému narušení.
Střední	3	Dopady jsou výrazné. Poskytování základní služby je výrazně ovlivněno, ale zároveň je možné ji nadále v omezené míře poskytovat.
Vysoká	4	Dopady jsou velmi výrazné. Poskytování základní služby je velmi výrazně ovlivněno, nicméně ještě nedochází k úplnému přerušení.
Velmi vysoká	5	Dopady jsou extrémní. Dochází k úplnému přerušení poskytování základní služby.

5. **Tabulka č. 3: Stupnice pro hodnocení rizik**

Úroveň	Hodnota	Popis
Přijatelná	1 až 2	Riziko je považováno za přijatelné. Není nutné přijímat žádná opatření.
Podmínečně přijatelná	3 až 12	Riziko je podmínečně přijatelné. Může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko považováno za přijatelné.
Nepřijatelná	13 až 25	Riziko je nepřijatelné a musí být zahájeny kroky k jeho odstranění.

Příloha č. 2

Hodnocení úrovně významnosti dopadů podle jednotlivých kritérií

(1) Kritérium A – Počet zasažených osob

Počet zasažených osob značí předpokládaný počet osob, které jsou nebo budou působením nežádoucí události ovlivněny.

(2) Kritérium B – Velikost zasaženého území

Velikost zasaženého území představuje předpokládané vymezení území, které je nebo bude působením nežádoucí události zasaženo.

(3) Kritérium C – Délka trvání

Délka trvání označuje předpokládanou dobu působení nežádoucí události až do obnovení poskytování základní služby.

(4) Kritérium D – Ekonomický dopad

Ekonomický dopad představuje předpokládanou finanční ztrátu subjektu kritické infrastruktury plynoucí z působení nežádoucí události.

(5) Kritérium E – Dopad na životní prostředí

Dopad na životní prostředí značí předpokládaný rozsah ovlivnění životního prostředí působením nežádoucí události. Slovní hodnocení na škále žádné až katastrofální zahrnuje následující rozsah dopadu:

a) žádné – dopady na životní prostředí nejsou identifikovány,

b) zanedbatelné – krátkodobé, lokální znečištění bez nutnosti zásahu; dopad nevyžaduje žádná nápravná opatření; není identifikován vliv na ekosystém nebo zdraví lidí,

c) nízké – mírné znečištění ovzduší, vody nebo půdy s identifikací lokálního vlivu na flóru a faunu bez trvalých následků; nápravná opatření nejsou složitá a nevyžadují finančně náročná řešení,

d) střední – výraznější kontaminace vyžadující dekontaminaci; dočasné narušení ekosystému nebo zemědělské produkce; možný vliv na zdraví obyvatel, zejména v podobě podráždění pokožky nebo alergie,

e) vážné – rozsáhlé znečištění s dopadem na vodní toky, půdu nebo ovzduší; úhyn živočichů, ohrožení chráněných druhů; nutnost zásahu specializovaných složek, vysoké náklady na obnovu, nebo

f) katastrofální – trvalé nebo nevratné poškození životního prostředí; ztráta biodiverzity, zničení přírodních lokalit; vysoké riziko pro zdraví obyvatel, dlouhodobé následky; mezinárodní důsledky.

(6) Kritérium F – Závislost jiných základních služeb

Závislostí jiných základních služeb se rozumí počet jiných základních služeb, které jsou na dané základní službě závislé, a mohlo by tak dojít k narušení poskytování těchto základních služeb.

(7) Kritérium G – Dopad na poskytování základní služby v jiném členském státě Evropské unie

Dopad na poskytování základní služby v jiném členském státě Evropské unie značí významný dopad nežádoucí události na kontinuitu poskytování základní služby v jiném členském státě Evropské unie nebo do takového státu. V případě významného dopadu nežádoucí události v šesti

nebo více členských státech nebo do těchto států je takováto nežádoucí událost považována za incident evropského významu.

Příloha č. 3

Stupnice pro hodnocení úrovně významnosti dopadů nežádoucí události

	Kritérium A	**Bodová hodnota A**	**Kritérium B**	**Bodová hodnota B**	**Kritérium C**	**Bodová hodnota C**	**Kritérium D**	**Bodová hodnota D**	**Kritérium E**	**Bodová hodnota E**	**Kritérium F**	**Bodová hodnota F**	**Kritérium G**	**Bodová hodnota G**
	Počet zasažených osob		***Velikost zasaženého území***		***Délka trvání***		***Ekonomický dopad***		***Dopad na životní prostředí***		***Závislost jiných základních služeb (ZS)***		***Dopad na poskytování základní služby v jiném ČS EU***	
	10 mil. a více	30	70 000 a více km^2	30	4 týdny a více	30	1 mld. Kč a více	30	katastrofální	30	70 a více ZS	30	6 a více ČS	30
	7 až méně než 10 mil.	28	50 000 až méně než 70 000 km^2	28	3 až méně než 4 týdny	28	750 mil. až méně než 1 mld. Kč	28	vážný	20	60 až 69 ZS	27	5 ČS	28
	5 až méně než 7 mil.	26	25 000 až méně než 50 000 km^2	26	2 až méně než 3 týdny	26	500 až méně než 750 mil. Kč	26	střední	15	50 až 59 ZS	24	4 ČS	25
	3 až méně než 5 mil.	24	10 000 až méně než 25 000 km^2	24	1 až méně než 2 týdny	24	250 až méně než 500 mil. Kč	24	nízký	5	40 až 49 ZS	21	3 ČS	20
	1 až méně než 3 mil.	22	5 000 až méně než 10 000 km^2	22	3 až méně než 7 dní	22	100 až méně než 250 mil. Kč	22	zanedbatelný	2	30 až 39 ZS	18	2 ČS	15

	500 tis. až méně než 1 mil.	20	1 000 až méně než 5 000 km^2	20	1 až méně než 3 dny	20	50 až méně než 100 mil. Kč	20	žádný	0	20 až 29 ZS	15	1 ČS	10
	250 až méně než 500 tis.	18	500 až méně než 1 000 km^2	18	12 až méně než 24 hodin	18	25 až méně než 50 mil. Kč	18			10 až 19 ZS	12	žádný	0
	100 až méně než 250 tis.	16	100 až méně než 500 km^2	16	6 až méně než 12 hodin	16	10 až méně než 25 mil. Kč	16			5 až 9 ZS	9		
	50 až méně než 100 tis.	13	50 až méně než 100 km^2	13	3 až méně než 6 hodin	13	5 až méně než 10 mil. Kč	13			2 až 4 ZS	6		
	10 až méně než 50 tis.	10	30 až méně než 50 km^2	10	1 až méně než 3 hodiny	10	1 až méně než 5 mil. Kč	10			1 ZS	3		
	5 až méně než 10 tis.	7	10 až méně než 30 km^2	7	30 až méně než 60 minut	7	500 tis. až méně než 1 mil. Kč	7			žádná	0		
	1 až méně než 5 tis.	5	5 až méně než 10 km^2	5	15 až méně než 30 minut	5	100 až méně než 500 tis. Kč	5						
	500 až méně než 1 tis.	3	2 až méně než 5 km^2	3	5 až méně než 15 minut	3	10 až méně než100 tis. Kč	3						
	do 500	2	do 2 km^2	2	1 až méně než 5 minut	2	do 10 tis. Kč	2						

	0	0	žádné	0	do 1 minuty	1	žádný	0						
Váhy	**0,20**		**0,20**		**0,15**		**0,15**		**0,10**		**0,10**		**0,10**	