…

VYHLÁŠKA
ze dne …

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

Ministerstvo vnitra stanoví podle § 14 odst. 6, § 15 odst. 2 a § 19 odst. 5 zákona č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon 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 a
c) parametry incidentu, podrobnosti rozsahu hlášených informací a způsob předávání informací o incidentu.

§ 2

Vymezení pojmů

Pro účely této vyhlášky se rozumí

a) metodikou písemný popis zvoleného přístupu, činnosti, postupu nebo východisek,
b) řízením rizik činnost subjektu kritické infrastruktury navazující na identifikaci a popis rizik v rámci provedení opatření pro jeho zvládnutí,
c) kontinuitou činností zachování nebo v určeném časovém rámci obnovení poskytování základní služby ve stanoveném rozsahu subjektem kritické infrastruktury při vzniku incidentu,
d) odezvou na incidenty soubor činností, které subjekt kritické infrastruktury vykonává v reakci na incident za účelem snížení jeho dopadů,
e) fyzickou bezpečností soubor opatření fyzické ochrany v rozsahu technických a organizačních opatření a ostrahy zaměřený zejména na ochranu majetku, osob a infrastruktury před neoprávněným přístupem, poškozením, krádeží nebo zničením,
f) technickými opatřeními mechanické a elektronické prostředky zajišťující objekt před narušením,
g) organizačními opatřeními soubor režimových opatření v rozsahu interních závazných a přesně definovaných pokynů, příkazů, omezení a postupů, sloužící ke stanovení režimu a způsobu použití opatření,
h) objektem budova nebo areál budov, stavba, technologické zařízení, komunikace, infrastruktura, pozemek nebo vnitřní prostor v budově, které jsou předmětem fyzické bezpečnosti,
i) bezpečnostním perimetrem prostorově vymezená oblast objektu,
j) řízením bezpečnosti pracovníků činnost subjektu kritické infrastruktury související s oprávněními a povinnostmi pracovníků v souvislosti se zajištěním bezpečnosti subjektu kritické infrastruktury,
k) řízením bezpečnosti dodavatelského řetězce činnost subjektu kritické infrastruktury související s opatřeními ve vztahu k dodavatelskému řetězci a nežádoucí událostí událost, která může narušit poskytování základní služby nebo jinou činnost subjektu kritické infrastruktury.

ČÁST DRUHÁ

POSOUZENÍ RIZIK SUBJEKTU KRITICKÉ INFRASTRUKTURY

§ 3

Kritická infrastruktura

Subjekt kritické infrastruktury

a) zpracuje metodiku pro charakteristiku své kritické infrastruktury, která obsahuje

1. postup pro identifikaci konkrétní kritické infrastruktury a
2. popis parametrů, na základě kterých k identifikaci došlo,

b) eviduje svou kritickou infrastrukturu a

c) na základě posouzení určuje a následně eviduje vzájemné vazby uvnitř kritické infrastruktury, přičemž posoudí existenci přímého nebo nepřímého vlivu vazby, možnost nahrazení vazby a časovou charakteristiku vazby.

§ 4

Posouzení rizik

(1) Subjekt kritické infrastruktury zpracuje posouzení rizik subjektu kritické infrastruktury v rámci dokumentace posouzení rizik. Při zpracování dokumentace posouzení rizik se vychází z ČSN ISO 31000, pokud není dále stanoveno jinak.

(2) Dokumentace posouzení rizik obsahuje

a) metodiku pro

1. identifikaci rizika,
2. analýzu rizika,
3. hodnocení rizika a
4. ošetření rizika,

b) popis techniky posuzování rizik a její aplikace podle přílohy B ČSN EN IEC 31010 a

c) posouzení rizik podle kritérií stanovených v metodice.

(3) 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 jeho kritickou infrastrukturu.

(4) Analýza rizik obsahuje rozbor povahy rizika a jeho vlastností. V rámci analýzy rizik se posuzuje

a) nejistota související s rizikem,

b) zdroj možného rizika,

c) předpokládaný následek související s rizikem,

d) pravděpodobnost výskytu rizika v souvislosti s nežádoucí událostí a

e) scénáře a opatření pro zvládání rizik s vyhodnocením jejich efektivnosti.

(5) 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 kritickou infrastrukturu podle tabulky č. 2 v příloze č. 1 k této vyhlášce.

(6) Součinem hodnot pravděpodobnosti a dopadu hrozby podle odstavce 5 subjekt kritické infrastruktury vypočítá úroveň rizika.

(7) 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 úroveň rizika 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 a nepřijatelná rizika.

(8) V rámci ošetření rizika subjekt kritické infrastruktury popíše způsob výběru a realizaci opatření k vyřešení nepřijatelného rizika.

(9) Subjekt kritické infrastruktury při zpracování posouzení rizik subjektu kritické infrastruktury vyhodnotí veškerá rizika související s činností člověka, přírodními vlivy a haváriemi, která by mohla vést k incidentu. Dále vyhodnotí rizika týkající se meziodvětvové nebo přeshraniční povahy, mimořádné události v oblasti veřejného zdraví, hybridních nebo jiných podobných hrozeb a teroristických útoků.

ČÁST TŘETÍ
PLÁN ODOLNOSTI

Náležitosti a způsob zpracování plánu odolnosti

§ 5

(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 schvaluje vedoucí organizační složky státu, guvernér České národní banky, statutární orgán právnické osoby nebo v případě kolektivního statutárního orgánu právnické osoby jeho pověřený člen, anebo subjektem kritické infrastruktury určený pracovník.

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

(4) Plán odolnosti se ukládá takovým způsobem, aby byl dostupný zaměstnancům v rozsahu odpovídajícím jejich pracovnímu zařazení a povinnostem.

§ 6

(1) Plán odolnosti se skládá z informační, operativní a podpůrné 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 struktury vedení organizace a její politiky,

d) plán spojení a

e) popis postupů využitých pro zpracování plánu odolnosti v návaznosti zejména na

1. právní předpisy a technické normy,
2. odvětvové metody a
3. vnitřní předpisy.

(3) Operativní část obsahuje

a) popis postupu, který byl využit pro identifikaci kritické infrastruktury,

b) popis postupu pro určení vazeb uvnitř kritické infrastruktury,

c) přehled nepřijatelných rizik, včetně posouzení meziodvětvových dopadů,

d) řízení rizik v rozsahu technických, bezpečnostních a organizačních opatření,

e) seznam kritických pracovníků,

f) popis zdrojů nezbytných k zajištění poskytování základní služby a

g) přehled kritických dodavatelů.

(4) Podpůrná část obsahuje

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

b) zásady manipulace s plánem odolnosti,

c) dokumentaci posouzení rizik,

d) geografické podklady a

e) dokumenty související s přijímáním opatření k zajištění odolnosti subjektu kritické infrastruktury.

§ 7

Pokud subjekt kritické infrastruktury zpracovává podle krizového zákona plán krizové připravenosti, obsahuje plán odolnosti dále

a) vymezení předmětu činnosti právnické nebo podnikající fyzické osoby a úkolů a opatření, které byly důvodem zpracování plánu krizové připravenosti,

b) přehled opatření vyplývajících z krizového plánu příslušného orgánu krizového řízení a způsob zajištění jejich provedení a

c) způsob zabezpečení akceschopnosti právnické nebo podnikající fyzické osoby pro zajištění provedení krizových opatření a ochrany činnosti právnické nebo podnikající fyzické osoby.

ČÁST ČTVRTÁ

OPATŘENÍ K ZAJIŠTĚNÍ ODOLNOSTI SUBJEKTU KRITICKÉ INFRASTRUKTURY

§ 8

Řízení rizik

(1) Subjekt kritické infrastruktury za účelem řízení rizik na základě výsledků provedeného hodnocení rizik vymezí opatření pro zvládání nepřijatelných rizik. Opatření osahuje

a) jeho popis, cíle a přínosy,

b) předpokládané lidské, finanční a technické zdroje pro zavedení opatření,

c) termín zavedení,
d) popis vazeb mezi riziky a opatřeními a
e) konkrétní způsob realizace.

(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, za jakých podmínek je možno vyloučit přijetí opatření.

(3) V souvislosti s opatřením pro řízení rizik se přijímají další opatření k zajištění odolnosti subjektu kritické infrastruktury v rozsahu
a) zpracování plánu zajištění kontinuity činností,
b) odezvy na incident,
c) zajištění fyzické bezpečnosti,
d) postupu pro řízení bezpečnosti pracovníků a
e) postupu pro řízení bezpečnosti dodavatelského řetězce.

§ 9

Zajištění kontinuity činností

(1) Subjekt kritické infrastruktury při přijímání opatření k zajištění kontinuity činností uplatní postupy a zásady stanovené ČSN ISO EN 22301, pokud není dále stanoveno jinak.

(2) Subjekt kritické infrastruktury pro zajištění kontinuity činností v rámci opatření zajišťujícího jeho odolnost zpracuje plán zajištění kontinuity činností, v rámci kterého
a) vypracuje metodiku, která obsahuje postup pro provedení analýzy dopadů,
b) provádí analýzu dopadů, která obsahuje vyhodnocení možných incidentů,
c) zohlední výsledky posouzení rizik subjektu kritické infrastruktury a
d) stanoví na základě výstupů analýzy dopadů a posouzení rizik subjektu kritické infrastruktury cíle zajištění kontinuity činností formou určení

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

e) stanoví postup řízení, který obsahuje naplnění cílů podle písmene d),
f) vypracuje a minimálně jednou za čtyři roky testuje plán kontinuity činností související s poskytováním základní služby a

g) provádí v návaznosti na povinnost podle písmene f) aktualizaci plánu kontinuity činností související s poskytováním základní služby.

§ 10

Odezva na incidenty

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

a) zpracuje vnitřní nastavení procesů a pravidel pro identifikaci, zaznamenání a vyhodnocení incidentů,

b) stanoví odpovědnost pracovníků za

1. identifikaci, zaznamenání a vyhodnocení incidentů a
2. koordinaci a zvládání incidentů,

c) definuje pravidla a postupy pro identifikaci, sběr, získání a uchování podkladů potřebných pro zpracování hlášení o incidentu,

d) zpracuje postup pro technická, bezpečnostní a organizační opatření pro odvrácení a zmírnění dopadu incidentu,

e) prošetří příčiny incidentu,

f) vede záznamy o incidentech a o jejich zvládání a

g) vyhodnotí účinnost řešení incidentu a stanoví nutná technická, bezpečnostní a organizační opatření k zamezení opakování incidentu, popřípadě aktualizuje stávající technická, bezpečnostní a organizační opatření k zajištění své odolnosti.

(2) Subjekt kritické infrastruktury v rámci opatření dále stanoví u

a) procesů, pravidel a postupů pro identifikaci, zaznamenání a vyhodnocení incidentů

1. interní postupy, podle kterých budou incidenty identifikovány, zaznamenány a vyhodnoceny a
2. nástroje a prostředky pro identifikaci, zaznamenání a vyhodnocení incidentu,

b) procesů, pravidel a postupů pro koordinaci a zvládání incidentů

1. interní postupy, podle kterých bude koordinace a zvládání incidentů probíhat a
2. způsob komunikace při koordinaci a zvládání incidentů a k tomu určené prostředky,

c) pravidel a postupů pro identifikaci, sběr, získání a uchování podkladů potřebných pro zpracování hlášení o incidentu

1. interní postupy, podle kterých bude identifikace, sběr, získání a uchování podkladů potřebných pro zpracování hlášení o incidentu probíhat, a
2. nástroje nebo prostředky pro identifikaci, sběr, získání a uchování podkladů potřebných pro zpracování hlášení o incidentu.

(3) V rámci opatření se pořizuje záznam o incidentu a o jeho zvládání, který 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,
f) důsledky incidentu,
g) informaci o případném přeshraničním dopadu incidentu,
h) počet a podíl uživatelů zasažených narušením poskytované základní služby,
i) dobu trvání narušení poskytování základní služby,
j) způsob jakým byl incident zvládnut a
k) návrh pro snížení rizika opakovaného vzniku incidentu.

§ 11

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 ohraničující oblast, ve které se nachází kritická infrastruktura,
b) může s ohledem na umístění kritické infrastruktury rozdělit bezpečnostní perimetr podle písmene a) do jednotlivých úrovní fyzické ochrany,
c) stanoví u každého bezpečnostního perimetru s ohledem na jeho úroveň fyzické ochrany technická a režimová opatření a
d) stanoví systém fyzické ochrany

1. k zamezení neoprávněnému vstupu,

2. k zamezení poškození, odcizení nebo zneužití kritické infrastruktury, neoprávněných zásahů do kritické infrastruktury a narušení poskytování základní služby,
3. k zajištění budov a jiných ohraničených prostor,
4. pro zajištění detekce narušení fyzického bezpečnostního perimetru a
5. k evidenci vstupů a přístupů do fyzického bezpečnostního perimetru.

(2) Subjekt kritické infrastruktury v souladu s výsledky posouzení rizik subjektu kritické infrastruktury v rámci opatření vyhodnotí potřebu zavedení technických opatření v rozsahu systému technické ochrany a elektrické požární signalizace.

(3) Systém technické ochrany tvoří soubor prostředků vnitřní a vnější ochrany, který zabraňuje, ztěžuje, detekuje nebo dokumentuje narušení fyzické ochrany. Mezi tyto prostředky patří, je-li to technicky možné nebo účelné, zejména

a) mechanické zábranné prostředky,
b) poplachový zabezpečovací a tísňový systém,
c) kamerové sledovací systémy,
d) systémy kontroly 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 video systémech,
i) dohledová a poplachová přijímací centra,
j) nouzové zvukové systémy a hlasová výstražná zařízení, nebo
k) bezpečnostní a nouzová osvětlení.

§ 12

Řízení bezpečnosti pracovníků

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

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

1. kategorií pracovníků vykonávajících kritické funkce,
2. přístupových práv k citlivým informacím, ke kritické infrastruktuře, popřípadě do jednotlivých kategorií bezpečnostních perimetrů,

3. kategorie osob, u nichž je vyžadováno ověření spolehlivosti,
4. požadavku na odbornou přípravu a kvalifikaci a
5. práva a povinnosti kritických pracovníků v rámci vedení,

b) vytvoří postup pro identifikaci osob stanovením

1. pozic, u kterých je ověřována spolehlivost,
2. způsobu kontroly dokumentů k prokázání totožnosti a bezúhonnosti a
3. osoby provádějící kontrolu dokumentů k prokázání totožnosti a bezúhonnosti,

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

d) zpracuje plán rozvoje bezpečnostního povědomí, který obsahuje

1. způsob poučení 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.

(2) 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 technických, bezpečnostních a organizačních opatření ze strany pracovníků a kritických pracovníků.

(3) Subjekt kritické infrastruktury vede o poučení a školení podle odstavce 1 písm. d) přehledy obsahující předmět poučení a školení a seznamu osob, které poučení a školení absolvovaly.

§ 13

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 dodavateli na základě výsledků posouzení rizik subjektu kritické infrastruktury,

b) informuje dodavatele o přijatých opatřeních souvisejících s dodavatelem a

c) označuje a 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) označení dodavatele za kritického dodavatele a
d) vyrozumění o skutečnosti, že dodavatel byl subjektem kritické infrastruktury označen za kritického dodavatele.

ČÁST PÁTÁ
IDENTIFIKACE A HLÁŠENÍ INCIDENTU

§ 14

Parametry incidentu

(1) Subjekt kritické infrastruktury za účelem identifikace incidentu vyhodnotí rizika pro jeho kritickou infrastrukturu v rámci posouzení rizik a identifikuje dopady nepřijatelných rizik. Na základě vyhodnocení rizik předběžně stanoví podle § 15 a příloh č. 2 a 3 k této vyhlášce možný rozsah dopadů 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 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,
g) dopad na ostatní členské státy Evropské unie a
h) přímý dopad na poskytování zdravotní péče.

§ 15

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 H 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 [%]; *Ki* je bodová hodnota i-tého kritéria podle přílohy č. 3 k této vyhlášce; *n* je počet kritérií; *Vi* je hodnota váhy i-tého kritéria podle přílohy č. 3 k této vyhlášce ; *Ki max* je maximální hodnota i-tého kritéria podle přílohy č. 3 k této vyhlášce.

(3) V případě naplnění prahové hodnoty 15 % úrovně významnosti dopadů nežádoucí události je nežádoucí událost považována za incident a parametry takové nežádoucí události za parametry incidentu.

§ 16

Formulář pro hlášení incidentu

(1) Incident se hlásí prostřednictvím formuláře pro hlášení incidentu subjektu kritické infrastruktury.

(2) Formulář pro hlášení incidentu subjektem kritické infrastruktury obsahuje

a) nadpis „Hlášení incidentu podle zákona o kritické infrastruktuře“,

b) jméno kontaktní osoby a kontaktní údaje a

c) identifikační údaje subjektu kritické infrastruktury, informace o poskytované základní službě, která byla zasažena incidentem, a druh hlášení v rozsahu

1. prvotního hlášení,
2. zprávy o pokroku a
3. závěrečné zprávy.

(3) Prvotní hlášení obsahuje

a) informace o incidentu, pokud jsou dostupné, v rozsahu

1. popisu,
2. data a času zjištění,
3. místa vzniku,
4. pravděpodobné příčiny vzniku a
5. stavu řešení incidentu,

b) informace vymezující dopad incidentu, v rozsahu

1. počtu uživatelů základní služby, kteří jsou nebo budou incidentem ovlivněni a jejich podíl na trhu v rámci dané základní služby, pokud je tato informace známá,
2. doby trvání narušení poskytování základní služby, po kterou bude působení incidentu zaznamenatelné,
3. území zasaženého narušením poskytování základní služby a
4. dopadu incidentu na poskytování základní služby v jiném členském státě Evropské unie nebo do takového státu.

(4) Zpráva o pokroku obsahuje

a) informace o nových skutečnostech týkajících se incidentu,
b) předpokládaný čas nutný pro vyřešení incidentu a
c) vysvětlení, z jakého důvodu incident stále trvá.

(5) Závěrečná zpráva obsahuje

a) shrnutí řešení incidentu, včetně jeho časové posloupnosti,
b) rozsah přijatých opatření a jejich účinnosti a informace podle odstavce 3 písm. b).

ČÁST ŠESTÁ
ÚČINNOST

§ 17

Tato vyhláška nabývá účinnosti dnem 1. dubna 2026.

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
Nízká	1	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední	2	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí 1 roku do 5 let.
Vysoká	3	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí 1 měsíce do 1 roku.
Kritická	4	Hrozba je velmi pravděpodobná až jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

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

Úroveň	Hodnota	Popis
Nízká	1	Dopady nejsou žádné nebo pouze zanedbatelné. Poskytování základní služby není ovlivněno.
Střední	2	Dopady jsou rozpoznatelné. Poskytování základní služby je ovlivněno, ale nedochází k výraznému narušení.
Vysoká	3	Dopady jsou významné. Poskytování základní služby je významně ovlivněno, nicméně nedochází k úplnému přerušení.

Kritická	4	Dopady jsou extrémní. Dochází k úplnému přerušení poskytování základní služby.

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

Úroveň	Hodnota	Popis
Nízká	1 až 4	Riziko je považováno za přijatelné.
Střední	5 až 8	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko přijatelné.
Vysoká	9 až 12	Riziko je dlouhodobě nepřijatelné a musí být zahájeny systematické kroky k jeho odstranění.
Kritická	13 až 16	Riziko je nepřijatelné a musí být neprodleně 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 (např. počet zákazníků nebo uživatelů závislých na poskytování základní služby).

(2) Kritérium B – Velikost zasaženého území

Velikost zasaženého území představuje předpokládané vymezení území, které je nebo bude působením nežádoucí události zasaženo (např. prostřednictvím osob závislých na poskytování základní služby).

(3) Kritérium C – Délka trvání

Délka trvání označuje předpokládanou dobu, po kterou bude působení nežádoucí události zaznamenatelné.

(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 (např. podráždění pokožky, 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 jiný členský stát Evropské unie

Dopad na jiný členský stát 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.

(8) Kritérium H – Přímý dopad na poskytování zdravotní péče

Přímý dopad na poskytování zdravotní péče značí skutečnost, zda v důsledku narušení poskytování základní služby dojde k případnému negativnímu ovlivnění zdravotní péče poskytované daným subjektem kritické infrastruktury.

Příloha č. 3

Stupnice pro hodnocení úrovně významnosti dopadů

	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**	**Kritérium H**	**Bodová hodnota H**
	Počet zasažených osob		***Velikost zasaženého území***		***Délka trvání***		***Ekonomický dopad***		***Dopad na životní prostředí***		***Závislost jiných základních služeb***		***Dopad na jiný členský stát EU (ČS)***		***Přímý dopad na poskytování zdravotní péče***	
	více než 10 mil.	30	celá ČR	30	více než 1 měsíc	30	více než 1 mld. Kč	30	katastrofální	30	více než 70	30	6 a více ČS	30	ano	30
	7 až 10 mil.	28	3/4 ČR	28	3 až 4 týdny	28	750 mil. až 1 mld. Kč	28	vážný	20	60 až 70	27	5 ČS	28	ne	0
	5 až 7 mil.	26	1/2 ČR	26	2 až 3 týdny	26	500 až 750 mil. Kč	26	střední	15	50 až 60	24	4 ČS	25		
	3 až 5 mil.	24	1/3 ČR	24	1 až 2 týdny	24	250 až 500 mil. Kč	24	nízký	5	40 až 50	21	3 ČS	20		
	1 až 3 mil.	22	2 kraje	22	3 až 7 dní	22	100 až 250 mil. Kč	22	zanedbatelný	2	30 až 40	18	2 ČS	15		
	500 tis. až 1 mil.	20	kraj	20	1 až 3 dny	20	50 až 100 mil. Kč	20	žádný	0	20 až 30	15	1 ČS	10		
	250 až 500 tis.	18	část kraje	18	12 až 24 hodin	18	25 až 50 mil. Kč	18			10 až 20	12	žádný	0		
	100 až 250 tis.	16	krajské město	16	6 až 12 hodin	16	10 až 25 mil. Kč	16			5 až 10	9				
	50 až 100 tis.	13	ORP	13	3 až 6 hodin	13	5 až 10 mil. Kč	13			2 až 5	6				
	10 až 50 tis.	10	město	10	1 až 3 hodiny	10	1 až 5 mil. Kč	10			1	3				
	5 až 10 tis.	7	část města	7	30 až 60 minut	7	500 tis. až 1 mil. Kč	7			0	0				
	1 až 5 tis.	5	obec	5	15 až 30 minut	5	100 až 500 tis. Kč	5								

	500 až 1 tis.	3	část obce	3	5 až 15 minut	3	10 až 100 tis. Kč	3								
	do 500	2	místní úroveň	2	1 až 5 minut	2	do 10 tis. Kč	2								
	0	0	žádné	0	do 1 minuty	1	žádný	0								
Váhy	**0,15**		**0,15**		**0,15**		**0,10**		**0,10**		**0,10**		**0,10**		**0,15**	