

Návrh tezí prováděcích právních předpisů k věcnému záměru zákona o odolnosti subjektů kritické infrastruktury

Část první

1. Nařízení vlády o základních službách a kritériích významnosti

Nařízení vlády o základních službách a kritériích významnosti navazuje na několik ustanovení v návrhu zákona o kritické infrastruktuře a stanovuje konkrétní základní služby, které prostřednictvím aktu v přenesené pravomoci Evropské komise a národních potřeb byly vyhodnoceny jako esenciální pro zajištění fungování České republiky. Stanovení kritérií pro tyto služby vychází téměř výhradně z obsahu směrnice CER. Stanovení kritéria významnosti ke každé základní službě v odvětví nebo pododvětví je zásadní pro identifikaci poskytovatele základní služby, který má povinnost informovat věcně příslušné ministerstvo, ústřední správní úřad nebo Českou národní banku a Ministerstvo vnitra, že spadá do regulace zákona a sdělit mu informace podle zákona o kritické infrastruktuře. Tento proces sebehodnocení slouží k určení tohoto poskytovatele subjektem kritické infrastruktury.

Tento dokument slouží jako rozpracované teze budoucího nařízení vlády 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.

Vláda stanoví podle § 8 odst. 4 a § 9 odst. 1 zákona č. XXX/XXXX Sb., o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře)

- a) základní služby v jednotlivých odvětvích nebo pododvětvích, a
- b) kritéria významnosti

Ve stanovených odvětvích nebo pododvětvích budou definovány základní služby včetně jejich kritérií významnosti, které umožní určit jednotlivé poskytovatele základních služeb. Kritéria významnosti budou mít stejně jako v případě dosavadních odvětvových kritérií podobu specifických technických, provozních a dalších hodnot definovaných pro každou základní službu zvlášť s ohledem na odvětví nebo pododvětví.

Kritéria významnosti budou určena v mezích směrnice CER a národních potřeb dle následujících parametrů:

- a) počet uživatelů, kteří jsou závislí na základní službě poskytované dotčeným poskytovatelem základní služby,
- b) rozsah, v němž jiná odvětví a pododvětví stanovená v příloze závisí na dotčené základní službě,
- c) možný dopad incidentů, pokud jde o jejich intenzitu a délku trvání, na ekonomické a společenské činnosti, životní prostředí, veřejnou bezpečnost a bezpečnost obecně nebo na zdraví obyvatelstva,
- d) tržní podíl poskytovatele základní služby na trhu s dotčenou základní službou či službami,
- e) území, které by mohlo být incidentem ovlivněno, včetně případných přeshraničních dopadů, s přihlédnutím ke zranitelnosti spojené se stupněm odloučení určitých typů území, jako jsou vzdálené regiony nebo horské oblasti,

- f) důležitost poskytovatele základní služby, pokud jde o udržování dostatečné úrovně dané základní služby, s přihlédnutím k dostupnosti alternativních způsobů poskytování této základní služby,
- g) jedinečnost poskytovatele základní služby, pokud jde o poskytování základní služby v jednotlivých odvětvích nebo pododvětvích nebo území

Jednotlivé parametry mohou být pro stanovení kritéria významnosti použity samostatně, nebo může být použita jejich kombinace.

Základní služby stanovené pro každé odvětví nebo pododvětví vycházejí z Nařízení komise v přenesené pravomoci ze dne 25. 7. 2023, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2022/2557 stanovením seznamu základních služeb aktu přenesené a z potřeb národní regulace na návrh věcně příslušných gestorů a Ministerstva vnitra.

Následující tabulka uvádí přehled jednotlivých odvětví a pododvětví základních služeb:

Odvětví	Pododvětví	Základní služba	Kritérium významnosti
Energetika	Elektřina	dodávky elektřiny	
		provoz, údržba a rozvoj distribuční soustavy elektřiny	
		provoz, údržba a rozvoj elektroenergetické přenosové soustavy	
		výroba elektřiny	
		služby nominovaného organizátora trhu s elektřinou	
		odezva strany poptávky	
		agregace elektřiny	
		ukládání energie	
	Dálkové vytápění a chlazení	poskytování dálkového vytápění nebo dálkového chlazení	
	Ropa	přeprava ropy	
		těžba ropy	
		rafinace a zpracování ropy	
		skladování ropy	
		správa zásob ropy, včetně nouzových zásob a specifických zásob ropy	
		skladování a přeprava pohonných hmot	
	Zemní plyn	dodávky zemního plynu	
		distribuce plynu	
		přeprava plynu	
		skladování plynu	
		provozování zařízení na zkapalněný zemní plyn (LNG)	
		těžba zemního plynu	
		nákup zemního plynu	
		rafinace a zpracování zemního plynu	
	Vodík	výroba vodíku	
		skladování vodíku	

		přeprava vodíku	
		distribuce vodíku	
Doprava	Letecká doprava	služby letecké dopravy využívané ke komerčním účelům (osobní a nákladní)	
		provoz, správa a údržba infrastruktury letišť a sítě letišť	
		služby řízení letového provozu	
	Železniční doprava	služby železniční dopravy (osobní a nákladní)	
		provoz, správa a údržba železniční infrastruktury, včetně osobních nádraží, nákladních terminálů, seřadovacích nádraží a středisek řízení provozu	
		provoz, správa a údržba zařízení železničních služeb	
		provoz, správa a údržba řízení železničního provozu, řízení a zabezpečení, jakož i telekomunikačních zařízení a systémů používaných pro řízení a zabezpečení	
	Vodní doprava	služby vnitrozemské, námořní a pobřežní vodní dopravy (osobní a nákladní)	
		provoz, správa a údržba přístavů a přístavních zařízení a provoz děl a zařízení v rámci přístavů, včetně doplňování paliva, nákladových operací, vyvazování, služeb osobní dopravy, sběru lodního odpadu a zbytků lodního nákladu, lodivodských služeb a služeb vlečných lodí	
		služby v lodní dopravě	
		služby vnitrozemské, námořní a pobřežní vodní dopravy (osobní a nákladní)	
	Silniční doprava	kontrola řízení provozu, včetně aspektů souvisejících s plánováním, řízením a správou silniční sítě, s výjimkou řízení provozu nebo provozování inteligentních dopravních systémů, pokud nejsou podstatnou součástí obecné činnosti veřejných subjektů	
		služby inteligentních dopravních systémů	
Veřejná přeprava	veřejné služby v přepravě cestujících po železnici a či jiným druhem drážní dopravy a po silnici		
Bankovníctví		přijímání vkladů	

		poskytování úvěrů	
Infrastruktura finanční trhů		provozování obchodního systému	
		provozování clearingových systémů	
Zdraví		poskytování služeb zdravotní péče	
		analýzy prováděné referenční laboratoří Evropské unie	
		výzkum a vývoj léčivých přípravků	
		výroba základních farmaceutických výrobků a základních farmaceutických přípravků	
		výroba zdravotnických prostředků považovaných za kriticky důležité v průběhu mimořádné situace v oblasti veřejného zdraví	
		distribuce léčivých přípravků	
Pitná voda		dodávka pitné vody a distribuce pitné vody s výjimkou distribuce vody určené k lidské spotřebě, pokud tato služba není podstatnou součástí obecné činnosti distributorů spočívající v distribuci jiných komodit a zboží	
Odpadní voda		odvádění, čištění a vypouštění odpadních vod s výjimkou odvádění, vypouštění nebo čištění městských odpadních vod, splašků nebo průmyslových odpadních vod, pokud nejsou podstatnou součástí obecných činností podniků	
Digitální infrastruktura	Služby vytvářející důvěru	poskytování služeb vytvářejících důvěru	
		poskytování služeb elektronické identifikace	
	Sítě a služby veřejných komunikací	poskytování veřejně dostupných služeb elektronických komunikací	
		poskytování veřejné sítě elektronických komunikací	
	Ostatní digitální služby a infrastruktura	poskytování a provozování služeb výměnných uzlů internetu	
		poskytování služeb systému překladu jmen domén (DNS) s výjimkou služeb souvisejících s kořenovými jmennými servery	
		provoz a správa registrů domén nejvyšší úrovně (TLD)	
		poskytování služeb cloud computingu	
		poskytování služeb datového centra	

		poskytování sítí pro doručování obsahu	
Veřejná správa		služby poskytované subjekty veřejné správy dle čl. 2 bodu 10 směrnice CER ústředních vlád vymezenými členskými státy v souladu s vnitrostátním právem	
Vesmír		provoz pozemních infrastruktur vlastněných, spravovaných a provozovaných členskými státy nebo soukromými subjekty a podporujících poskytování služeb využívajících kosmického prostoru, s výjimkou poskytovatelů veřejných sítí elektronických komunikací	
Výroba, zpracování a distribuce potravin		rozsáhlá průmyslová výroba a zpracování potravin	
		služby dodavatelského řetězce potravin, včetně skladování a logistiky	
		velkoobchodní distribuce potravin	
Bezpečnost	Nouzové služby		
	Vnitřní pořádek		
	Monitorování radiační situace		
	Hydrometeorologická výstražná služba		
	Obranný průmysl		
Odpadové hospodářství			
Státní hmotné rezervy			

2. Nařízení vlády o obsahu Strategie pro posílení odolnosti subjektů kritické infrastruktury

Nařízení vlády o základních službách a kritériích významnosti navazuje na několik ustanovení v novém Zákoně o kritické infrastruktuře a stanovuje obsah Strategie pro posílení odolnosti subjektů kritické infrastruktury. Cílem Strategie je stanovení strategických cílů a opatření s cílem dosáhnout vysoké úrovně odolnosti subjektů kritické infrastruktury na základě relevantních stávajících vnitrostátních a odvětvových strategií, plánů nebo obdobných dokumentů. Obsah strategie vychází téměř výhradně z obsahu směrnice CER. Ministerstvo vnitra je podle § 6 odst. 1 písm. b) povinno, za součinnosti ministerstev, jiných ústředních správních úřadů a České národní banky, zpracovat Strategii pro posílení odolnosti subjektů kritické infrastruktury a aktualizovat ji nejméně jednou za 4 roky. Ministerstvo vnitra předkládá Strategii vládě, která ji následně schvaluje svým usnesením. Zároveň předloží Strategii Evropské komisi do tří měsíců od jejího schválení k posouzení. Cílem tohoto dokumentu je centrální stanovení postupů k zajištění kontinuálního poskytování základních služeb v České republice.

Tento dokument slouží jako rozpracované teze budoucího nařízení vlády 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.

Vláda schvaluje podle § 4 zákona č. XXX/XXXX Sb., o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře) za účelem zvyšování odolnosti subjektů kritické infrastruktury Strategii pro posílení odolnosti subjektů kritické infrastruktury a za tímto účelem stanoví obsah této Strategie.

Strategie bude obsahovat následující oblasti:

- a) strategické cíle a priority za účelem posílení celkové odolnosti subjektů kritické infrastruktury s přihlédnutím k přeshraniční a meziodvětvové jednostranné i vzájemné závislosti,
- b) správní rámec pro naplnění strategických cílů a priorit, včetně popisu úlohy a odpovědností různých orgánů, subjektů kritické infrastruktury a dalších stran zapojených do provádění této strategie,
- c) popis opatření nezbytných k posílení celkové odolnosti kritických subjektů, včetně popisu posouzení rizik podle článku 5 směrnice CER, v případě České republiky se bude jednat o odkaz na Posouzení rizik ČR, které se zpracovává podle krizového zákona,
- d) popis postupu, jak jsou určovány subjekty kritické infrastruktury,
- e) popis procesu podpory subjektů kritické infrastruktury, včetně opatření na posílení spolupráce mezi veřejným sektorem na jedné straně a soukromým sektorem a veřejnými a soukromými subjekty na straně druhé,
- f) seznam hlavních orgánů a příslušných zúčastněných stran jiných než subjektů kritické infrastruktury zapojených do provádění strategie,
- g) rámec politik pro koordinaci mezi příslušnými orgány podle této směrnice (dále jen „příslušné orgány“) a Národním úřadem pro kybernetickou a informační bezpečnost podle směrnice (EU) 2022/2555 pro účely sdílení informací o kybernetických bezpečnostních rizicích, kybernetických hrozbách a kybernetických incidentech, stejně jako o jiných než kybernetických rizicích, hrozbách a incidentech a výkonu úkolů v oblasti dohledu, a
- h) popis již zavedených opatření, jejichž cílem je usnadnit malým a středním podnikům plnění povinností ve smyslu přílohy doporučení Komise 2003/361/ES(31), které dotčený členský stát určil jako subjekty kritické infrastruktury.

3. Vyhláška o náležitostech a zpracování plánu odolnosti, posouzení rizik, obsahu a rozsahu opatření k zajištění odolnosti a podrobnostech ověřování spolehlivosti

Vyhláška Ministerstva vnitra navazuje na několik ustanovení v návrhu zákona o kritické infrastruktuře a stanovuje podrobnosti ke zpracování plánu odolnosti a posouzení rizik subjektu kritické infrastruktury, jím přijímaným opatření k zajištění odolnosti a specifika pro oblast ověřování spolehlivosti. Subjekt kritické infrastruktury má povinnost zpracovat posouzení rizik subjektu kritické infrastruktury do 9 měsíců a plán odolnosti do 10 měsíců od doručení informace o zařazení na seznam subjektů kritické infrastruktury, aktualizace obou dokumentů se následně provádí minimálně každé čtyři roky. Obsah dokumentace, včetně rozsahu opatření, vychází téměř výhradně z obsahu směrnice CER.

Vzhledem k narůstajícímu riziku, že pracovníci subjektu kritické infrastruktury nebo jeho významného dodavatele zneužijí například svá přístupová práva v rámci organizace subjektu kritické infrastruktury k poškození a způsobení škody, jsou v zákoně o kritické infrastruktuře upřesněny podmínky, podle nichž je subjektům kritické infrastruktury umožněno v řádně odůvodněných případech a s přihlédnutím k Posouzení rizik ČR podávat žádosti o ověření spolehlivosti u osob, které spadají do určitých kategorií jejich pracovníků. Ze směrnice CER vychází způsob ověřování totožnosti a zjištění trestně-právní bezúhonnosti formou výpisu z rejstříku trestů. V rámci národní regulace je ve zvláštních případech využít institut citlivé činnosti.

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.

Ministerstvo vnitra podle § 13 odst. 6, § 15 odst. 2 a § 17 odst. 4 zákona č. XXX/XXXX Sb., o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře) stanoví náležitosti a způsob zpracování plánu odolnosti a posouzení rizik subjektu kritické infrastruktury, obsah a rozsah opatření k zajištění odolnosti subjektu kritické infrastruktury a funkce nezbytné pro zajištění poskytování základní služby, jejichž výkon je citlivou činností vybraná odvětví nebo pododvětví.

Posouzení rizik

V případě posouzení rizik subjektu kritické infrastruktury budou zohledněna veškerá příslušná přírodní rizika a rizika způsobená člověkem, která by mohla zapříčinit incident, včetně rizik meziodvětvové nebo přeshraniční povahy, havárií, přírodních katastrof, mimořádných událostí, hybridních hrozeb či jiných antagonistických hrozeb. Posouzení rizik subjektu kritické infrastruktury zohlední i míru závislosti jiných odvětví stanovených v příloze na základní službě poskytované subjektem kritické infrastruktury a míru závislosti subjektu kritické infrastruktury na základních službách poskytovaných subjekty v těchto jiných odvětvích, a to v příslušných případech včetně odvětví v sousedních členských státech a případně třetích zemích. Základem pro posouzení rizik subjektu kritické infrastruktury by pak mělo být posouzení rizik České republiky, které bude zpracováváno podle návrhu novely krizového zákona. Zároveň, pokud subjekty kritické infrastruktury provedly jiná posouzení rizik nebo vypracovaly dokumenty podle povinností stanovených v jiných právních předpisech, které jsou relevantní pro posouzení rizik subjektu kritické infrastruktury, mohou tato posouzení a dokumenty použít ke splnění požadavku na zpracování posouzení rizik subjektu kritické infrastruktury.

Plán odolnosti a opatření k zajištění odolnosti

V plánu odolnosti subjektu kritické infrastruktury budou rozpracována a popsána technická, bezpečnostní a organizační opatření, která jsou vhodná a přiměřená rizikům, jimž subjekt kritické infrastruktury čelí, a to za účelem předcházení incidentům, zajištění odolnosti a řízení kontinuity činnosti. Konkrétně bude v rámci plánu odolnosti řešeno předcházení vzniku incidentů, zajištění přiměřené fyzické ochrany kritické infrastruktury, dále opatření zaměřená na odezvu a odolávání důsledkům incidentu a jejich zmírňování. Součástí budou také opatření související se zotavením subjektu kritické infrastruktury z následků incidentu a to včetně opatření pro zajištění kontinuity činnosti. Součástí opatření k řízení rizik bude plánování věcných zdrojů a dalších nástrojů, ke kterému je subjekt oprávněn podle § 13 odst. 3 zákona.

Obsahem plánu odolnosti dále budou opatření týkající se řízení bezpečnosti zaměstnanců a to i ve vazbě na mechanismus ověřování spolehlivosti. Spolu s personálními opatřeními budou také řešena opatření k zajištění odborné přípravy zaměstnanců a zvyšování povědomí o přijatých opatřeních a možných rizicích. Stejně jako u posouzení rizik subjektu kritické infrastruktury, i v případě plánu odolnosti může subjekt kritické infrastruktury ke splnění požadavku na zpracování plánu odolnosti použít obdobnou dokumentaci zpracovávanou podle povinností stanovených v jiných právních předpisech, která je relevantní pro plán odolnosti.

Struktura a obsah plánu odolnosti nad rámec stanovený směrnicí CER bude vycházet i z plánu kontinuity podnikání podle ISO 22301.

Opatření k zajištění odolnosti, které vycházejí ze zákona, budou rozpracována následujícím způsobem:

- a) preventivních opatření k předcházení vzniku incidentů,
- b) opatření fyzické bezpečnosti,
- c) opatření k řízení rizik a odezvy na incidenty,
 - součástí plánování věcných zdrojů podle § 13 odst. 3
- d) opatření pro zajištění kontinuity činnosti,
- e) opatření k řízení bezpečnosti pracovníků,
- f) opatření k řízení bezpečnosti dodavatelského řetězce.

Ověřování spolehlivosti

V souvislosti s ověřováním spolehlivosti stanoví vyhláška okruh klíčových funkcí vykonávajících citlivou činnost pro vybraná odvětví nebo pododvětví. Pro výkon činnosti těchto funkcí bude vyžadován platný doklad o bezpečnostní způsobilosti fyzické osoby, který vydává Národní bezpečnostní úřad. Vždy se bude jednat o funkci manažera kritické infrastruktury a dále funkce, které stanoví gestor odvětví nebo pododvětví ve spolupráci s Ministerstvem vnitra a Národním bezpečnostním úřadem. Byla prioritizována taková odvětví nebo pododvětví, která mají vysoký plošný dopad na obyvatelstvo v případě úmyslného narušení základní služby ze strany pracovníka.

V rámci funkcí se bude jednat zpravidla o pracovníky technických dispečinků, osob s přístupem do životně důležitých prostor k zajištění poskytování základní služby nebo výkon funkce statutárního orgánu.

4. Vyhláška k podrobnostem hlášení incidentů

Vyhláška Ministerstva vnitra navazuje na několik ustanovení v novém Zákoně o kritické infrastruktuře a stanovuje mechanismus pro oznamování incidentů, který by příslušným orgánům umožnil na incidenty reagovat rychle a odpovídajícím způsobem a mít komplexní přehled o dopadu, povaze, příčinách a možných důsledcích incidentů, které subjekty kritické infrastruktury řeší. Náležitosti hlášení incidentů, včetně dokumentace s tím spojené, vychází téměř výhradně z obsahu směrnice CER.

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.

Ministerstvo vnitra podle § 19 odst. 5 zákona č. XXX/XXXX Sb., o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře) stanoví parametry incidentu, který podléhá hlášení, podrobnosti rozsahu hlášených informací, způsob předávání informací o incidentu, podrobnosti k prvotnímu hlášení a závěrečné zprávě.

Součástí této vyhlášky bude stanovení prahových hodnot dopadu na poskytování základní služby sloužících k identifikaci incidentu. Ukazatelem pro určení těchto prahových hodnot bude kritérium významnosti u každé základní služby.

Hlášení incidentu bude primárně probíhat prostřednictvím formuláře v Portálu kritické infrastruktury, do kterého dotčený subjekt kritické infrastruktury zadá požadované informace. Tyto informace by měly obsahovat základní údaje o vzniklém incidentu, jako jsou typ incidentu a čas a místo jeho vzniku, způsobené poškození infrastruktury subjektu kritické infrastruktury a rozsah narušení poskytované základní služby nebo poskytovaných základních služeb.

Parametry incidentu

Za incident bude považována taková událost, která bude svým rozsahem splňovat parametry incidentu. Parametry incidentu tak budou sloužit k rozlišení incidentů, které budou subjekty povinny hlásit. Zároveň budou definovány prahovými hodnotami těchto údajů:

- poměrnou částí vůči kritériu významnosti,
- druhem incidentu,
- zasaženou infrastrukturou,
- předpokládaným počtem uživatelů zasažených narušením,
- předpokládanou dobu trvání narušení,
- případným přeshraničním dopadem.

Hlášení a způsob předávání informací o incidentu

Subjekt kritické infrastruktury by měl bez zbytečného odkladu oznamovat Ministerstvu vnitra incidenty, které významně narušují nebo mohou významně narušit poskytování základních služeb. Hlášení bude obsahovat tyto údaje:

- a) počet a podíl uživatelů zasažených narušením poskytované základní služby,
- b) dobu trvání narušení,
- c) území zasažené narušením, a
- d) povahu, příčinu a možné důsledky incidentu, včetně informací nezbytných ke stanovení případného přeshraničního dopadu incidentu.

V případě, že subjekt kritické infrastruktury není z důvodu řešení incidentu schopen zaslat požadované informace v plném rozsahu, předloží prvotní oznámení nejpozději 24 hodin poté, co se o incidentu dozvěděl. Prvotní oznámení by mělo obsahovat pouze informace, které jsou zcela nezbytné k vyrozumění příslušného orgánu o incidentu, a které subjektu kritické infrastruktury umožňují v případě potřeby požádat o pomoc.

Hlášení incidentu a veškeré předávání informací o něm bude probíhat primárně prostřednictvím Portálu kritické infrastruktury. Záměrem je včasné a cílené vyrozumění Ministerstva vnitra a věcně příslušných ministerstev nebo jiných ústředních správních úřadů o vzniku incidentu.

Prvotní hlášení

Prvotní hlášení slouží k rychlému vyrozumění o vzniku incidentu. Bude obsahovat pouze informace, **kteřé jsou zcela nezbytné k vyrozumění příslušného orgánu o incidentu, a kterež subjektu KI umožňují v případě potřeby požádat o pomoc.**

Obsah prvotního hlášení incidentu:

- odhadovaný počet a podíl uživatelů zasažených narušením,
- odhadovaná doba trvání narušení,
- přibližný rozsah území zasaženého narušením s přihlédnutím k tomu, zda je toto území geograficky izolované,
- současná povaha incidentu,
- předpokládaná příčina vzniku incidentu,
- možné důsledky incidentu,
- informace nezbytné ke stanovení případného přeshraničního dopadu incidentu.

Závěrečná zpráva

Závěrečná zpráva o incidentu bude do 30 dnů po předložení prvotního hlášení zaslána prostřednictvím Portálu kritické infrastruktury Ministerstvu vnitra, které je bude sdílet s věcně příslušným ministerstvem nebo jiným ústředním správním úřadem. Její podstatou je podrobný popis nastalého incidentu, o kterém bylo Ministerstvo vnitra informováno v prvotním hlášení. Obsahem závěrečné zprávy bude:

- datum a čas vzniku incidentu,
- celkový počet a podíl uživatelů zasažených narušením,
- doba trvání narušení,
- celkový rozsah území zasaženého narušením,
- povaha incidentu,
- příčina vzniku incidentu,
- přímé důsledky incidentu,
- případný přeshraniční dopad incidentu.

V případě, že incident trvá po dobu delší, než 30 dnů, zašle subjekt kritické infrastruktury tzv. zprávu o pokroku, která bude obsahovat další doplňující informace ve vztahu k prvotnímu hlášení.

5. Vyhláška o Portálu kritické infrastruktury

Vyhláška Ministerstva vnitra navazuje na několik ustanovení v návrhu zákona o kritické infrastruktuře a stanovuje způsob výměny informací mezi zainteresovanými subjekty a současně upravuje technické a procesní náležitosti technického řešení automatizace a elektronizace procesů subjektu kritické infrastruktury, Ministerstva vnitra a věcně příslušných ministerstev, jiných ústředních správních úřadů nebo České národní banky, které jsou spojeny s výkonem většiny agend podle nového Zákona kritické infrastruktury.

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.

Ministerstvo vnitra podle § 20 odst. 9 zákona č. XXX/XXXX Sb., o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře) stanoví Formu a způsob zpracování informací, dat, údajů a evidencí vkládaných do Portálu kritické infrastruktury, stejně jako technické a organizační podmínky používání Portálu kritické infrastruktury.

Přístup do Portálu kritické infrastruktury a jeho následné používání se provádí prostřednictvím webového rozhraní. Portál kritické infrastruktury je neveřejný a přihlašuje se do něj prostřednictvím přidělených přihlašovacích údajů a ověření identity. Portál je modulem tzv. informačního systému krizového řízení a využívá tak jeho infrastruktury a procesy zabezpečení.

Portál bude získávat a zpracovávat informace o poskytovatelích základních služeb potřebné k jejich určení subjektem kritické infrastruktury. Data budou zadávána prostřednictvím formulářů s filtry. Prostřednictvím Portálu budou subjekty určovány a vedena s nimi elektronická komunikace. Portál bude sloužit i k dalšímu plnění povinností subjektů KI a budou v něm vedeny informace, data, údaje nebo evidencí podle § 5 odst. 1 písm. e), § 5 odst. 2, § 6 písm. e), § 8, § 11, § 12, § 18 a § 21. Portál bude rovněž schopen vzájemné dobrovolné komunikace mezi subjekty navzájem a mezi subjekty a věcně příslušnými orgány.

Vyhláška dále stanoví formální náležitosti vybraných úkonů podle Zákona o kritické infrastruktuře, zejména pak podobu formulářů.

Část druhá

Návrh tezí nařízení vlády k provedení zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů

Jedná se o teze nařízení, jehož přesná podoba bude dále projednávána a modifikována v rámci přípravy tohoto podzákonného předpisu.

Toto nařízení vlády je vydáváno na základě zmocnění uvedeném v § 40 krizového zákona a nahradí nařízení vlády č. 462 ze dne 22. listopadu 2000 k provedení § 27 odst. 8 a § 28 odst. 5 zákona č.240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.

Nařízení vlády bude upravovat

1. **Obsahové náležitosti, členění a způsob zpracování posouzení rizik České republiky, krizových plánů, karty obce, plánů krizové připravenosti a karty subjektu.**

Nařízení vlády bude definovat obsahové náležitosti, členění a způsob zpracování jak nově zpracovávané dokumentace podle krizového zákona (např. krizový plán ČR), tak dokumentace, která je již zpracovávána (např. krizový plán kraje), avšak na základě zkušeností z aplikační praxe je třeba tuto dokumentaci více zjednodušit a přiblížit potřebám jejího využití při přípravě a řešení krizových situací.

Zcela nově budou stanoveny obsahové náležitosti, členění a způsob zpracování **posouzení rizik ČR.**

Jedná se o dokument, který bude identifikovat hrozby pro ČR, který také bude obsahovat analýzu těchto rizik a jejich hodnocení (v současnosti je obdobným dokumentem Analýza hrozeb pro Českou republiku, kterou schválila vláda usnesením č. 369 ze dne 27. dubna 2016). S ohledem na nové požadavky z úrovně Evropské unie (např. Směrnice CER), je třeba tuto analýzu dále rozšířit zejména o podrobnější zhodnocení dopadů na kritickou infrastrukturu a také o zohlednění meziodvětvových závislostí.

V souladu s výstupy posouzení rizik bude zpracováván **krizový plán ČR.** Jedná se o nový dokument na národní úrovni, jehož obsahem bude zejména stanovení komunikačních a informačních toků na ústřední úrovni (případně předávání informací na další úroveň), opatření pro řešení krizových situací identifikovaných v posouzení rizik ČR a stanovení gestorů pro jejich provedení.

Krizový plán ministerstva nebo jiného ústředního správního úřadu, krizový plán kraje, krizový plán obce s rozšířenou působností jsou dokumenty, které jsou již zpracované a jejichž obsahové náležitosti a způsob zpracování upravuje nařízení vlády č. 462/2000 Sb. Zde se předpokládají pouze dílčí úpravy obsahu této dokumentace, které vychází ze zkušeností z aplikační praxe.

Nově zpracovávaným dokumentem je **karta obce.** Nařízení vlády stanoví obsahové náležitosti, členění a způsob zpracování této dokumentace, kterou bude zpracovávat obecní úřad a je primárně určena pro starostu dané obce. Jedná o velice stručný dokument – kartu, která bude pomůckou pro starostu a bude mu přinášet základní údaje potřebné pro řešení mimořádných událostí či krizových situací na území obce (např. základní přehled rizik na území, důležité kontakty a potřebné postupy apod.). Zá účelem jednotnosti zpracování této dokumentace bude vytvořen jednotný vzor.

Plán krizové připravenosti krajského úřadu a plán krizové připravenosti obecního úřadu obce s rozšířenou působností je dokument, který slouží k zajištění vlastního fungování a plnění potřebných úkolů příslušných úřadů za mimořádných událostí a krizových situací. Nařízení vlády stanoví základní obsahový rámec tohoto dokumentu a způsob jeho zpracování

Právnícké a podnikající fyzické osoby, které zajišťují plnění opatření vyplývajících z krizového plánu podle § 29 odst. 1 krizového zákona, jsou nově povinny zpracovávat **kartu subjektu**. Jedná se o dokumentaci, která nahradí původně zpracovávaný plán krizové připravenosti. Karta subjektu bude však stručnějším dokumentem, ve kterém bude stanoveno, jaký úkol z krizového plánu subjekt plní a jakým způsobem jej bude zajišťovat, popř. zda-li má nějaké požadavky na orgány krizového řízení, bez nichž není možné opatření plnit.

2. Nařízení vlády stanoví minimální obsah činnosti bezpečnosti rady kraje a bezpečnostní rady obce s rozšířenou působností a také základní složení těchto orgánů a také minimální obsah činnosti ústředního krizového štábu, krizového štábu kraje a krizového štábu obce s rozšířenou působností a také základní složení těchto orgánů.

Další oblastí řešenou v tomto nařízení vlády bude obsah činnosti a složení bezpečnostních rad a krizových štábů. Základ této oblasti bude přímo vycházet z již existujícího obsahu činnosti a složení podle stávajícího znění. Reflektována však bude identifikovaná potřeba zajištění určité míry adaptability složení těchto orgánů ve specifických podmínkách jednotlivých územně samosprávných celků. Nově bude definována role sekretariátu těchto orgánů, čímž dojde zároveň ke sjednocení základní struktury krizových štábů krajů a obcí s rozšířenou působností s ústředním krizovým štábem.