Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č.J. NEPŘIDĚLENO • BRNO • 22. PROSINCE 2022

VERZE DOKUMENTU: 1.1

PRÁVA A POVINNOSTI SUBJEKTŮ KRITICKÉ INFORMAČNÍ INFRASTRUKTURY

Specifická práva a povinnosti podle krizového zákona
nad rámec povinností podle zákona o kybernetické bezpečnosti

Obsah

1 Úvod

Tento dokument je určen především správcům kritické informační infrastruktury, tedy povinným osobám podle § 3 písm. c) a d) zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „zákon o kybernetické bezpečnosti“). Obsahuje shrnutí práv a povinností, které těmto správcům kritické informační infrastruktury vyplývají ze zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (dále jen „krizový zákon“), a pohled Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „Úřad“), jako orgánu krizového řízení majícího nad těmito subjekty v dané agendě působnost, na způsob plnění zákonných povinností a soulad s požadavky zákona o kybernetické bezpečnosti.

V případě dotazů se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost

Mučednická 1125/31

616 00 Brno – Žabovřesky

E-mail: regulace@nukib.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

2 Obecná východiska

Jednou z povinností Úřadu je určovat v souladu s § 22 písm. m) a n) zákona o kybernetické bezpečnosti prvky kritické infrastruktury nebo zasílat návrh těchto prvků Ministerstvu vnitra, pokud jde o organizační složky státu. Tím je Úřad postaven do role orgánu krizového řízení podle § 9 odst. 3 písm. c) a d) krizového zákona.

Pravomoc Úřadu je však omezena a může určovat či navrhovat pouze takové prvky kritické infrastruktury, které naplňují některé z odvětvových kritérií daných v odvětví VI. Komunikační a informační systémy, oblast G. Kybernetická bezpečnost podle nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury (dále jen „nařízení vlády“). Každý prvek nebo systém prvků kritické infrastruktury, který byl určen na základě takového kritéria, se označuje jako **„kritická informační infrastruktura“.**

Orgány a osoby, které vůči takto určené kritické informační infrastruktuře naplní definice správce v souladu s § 2 zákona o kybernetické bezpečnosti, můžeme pro potřeby tohoto dokumentu souhrnně označit jako **„subjekty kritické informační infrastruktury“**.

Subjektům kritické informační infrastruktury jsou uloženy povinnosti zejména zákonem o kybernetické bezpečnosti – musí zavádět bezpečnostní opatření, hlásit kontaktní údaje a kybernetické bezpečnostní incidenty apod.

Protože se však v případě kritické informační infrastruktury zároveň stále jedná o prvky kritické infrastruktury, jsou subjektům kritické informační infrastruktury uložena práva a povinnosti také krizovým zákonem.

Z tohoto důvodu dokument pracuje také s označením „subjekt kritické infrastruktury“, protože povinnosti vyplývající z krizového zákona nejsou odlišné pro subjekty kritické informační infrastruktury a ostatní subjekty kritické infrastruktury.

Pojem „subjekt kritické **informační** infrastruktury“ pak dokument používá především tam, kde má za cíl zdůraznit některé detaily specifické pro tuto podmnožinu.

3 Práva subjektů kritické infrastruktury z krizového zákona

Subjekt kritické infrastruktury požívá jistých výhod ze svého postavení v rámci krizového zákona, a to zejména:

- **možnost přednostního zásobování** při nouzovém stavu (příp. i stavu nebezpečí),[1]
- **omezení povinnosti poskytnout věcné prostředky** k řešení krizového stavu (poskytnutím prostředků nesmí dojít k narušení funkce prvku kritické infrastruktury),[2]
- **osvobození od pracovní povinnosti a pracovní výpomoci pro zaměstnance** subjektu kritické infrastruktury, kteří se podílejí na zajištění funkce prvku kritické infrastruktury[3]

3.1.1 Možnost přednostního zásobování při nouzovém stavu a stavu nebezpečí

Subjekt kritické infrastruktury přijímá opatření na ochranu prvku kritické infrastruktury. Taková opatření spočívají také v zajištění dostatečných dodávek pro jeho správné fungování. V případě krizové situace, kdy tato opatření selžou nebo jsou nedostatečná, může nastoupit tzv. přednostní zásobování. Podle krizového zákona mohou být po dobu trvání nouzového stavu subjekty kritické infrastruktury přednostně zásobovány. Stejně tak tomu může být i v případě stavu nebezpečí, kdy krizový zákon však toto přednostní zásobování podmiňuje tím, že může být prováděno jen „v nezbytném rozsahu“ (rozsah podpory za nouzového stavu krizový zákon neupravuje). Přednostní zásobování může nařídit vláda v případě nouzového stavu a hejtman za stavu nebezpečí, konkrétní postupy.

S ohledem na povahu kritické informační infrastruktury lze očekávat, že přednostní zásobování se v jejím případě bude týkat zejména pohonných hmot k zajištění chodu záložních zdrojů napájení elektrickou energií. Detaily provedení a nařízení přednostního zásobování se budou vždy lišit v závislosti na dané situaci. Přednostní zásobování může v případě potřeby (kdy by hrozilo narušení funkce prvků kritické infrastruktury) nařídit vláda jako krizové opatření během nouzového stavu, nebo v nezbytném rozsahu také hejtman za stavu nebezpečí.

3.1.2 Omezení povinnosti poskytnout věcné prostředky k řešení krizového stavu

Obecně je možné v rámci krizových situací uložit právnickým nebo podnikajícím fyzickým osobám povinnost poskytnout věcné prostředky potřebné k řešení dané krizové situace. Tato povinnost je uložena výzvou oprávněného orgánu krizového řízení. Pojem „věcné prostředky“ lze v tomto případě vnímat velmi široce, protože se může jednat o jakékoliv movité i nemovité věci nebo také služby.

Stejně jako v případě jiných osob, také subjekty kritické infrastruktury jsou obecně povinny takové věcné prostředky na výzvu poskytnout. Na rozdíl od ostatních subjektů u nich však existuje

[1] § 6 odst. 2 písm. f) bod 3 krizového zákona
[2] § 29 odst. 3 krizového zákona
[3] § 32 odst. 2 krizového zákona

možnost neposkytnout takové věcné prostředky, jejichž poskytnutím by došlo nebo mohlo dojít k narušení funkce prvku kritické infrastruktury.

V případě kritické informační infrastruktury je zde jistě na místě zvážit pro aplikaci této výjimky použití informací uvedených v evidenci aktiv, kterou subjekt kritické informační infrastruktury vede podle § 4 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). Tímto postupem lze pak zajistit, že je výjimka aplikována účelně a ve vztahu k aktivům, která jsou pro subjekt kritické infrastruktury a jeho provoz vitální.

3.1.3 Osvobození od pracovní povinnosti a pracovní výpomoci pro zaměstnance subjektu kritické infrastruktury, kteří se podílejí na zajištění funkce prvku kritické infrastruktury

Obecně je možné v rámci krizových situací nařídit právnickým nebo podnikajícím fyzickým pracovní povinnost nebo pracovní výpomoc. Pracovní povinností se rozumí povinnost fyzické osoby vykonávat po nezbytně nutnou dobu určenou práci, která je nutná pro řešení krizové situace a kterou je tato osoba povinna konat v místě určeném orgánem krizového řízení. Pracovní výpomoc je pak konání určené práce krátkodobějšího a nárazového rázu.

Zaměstnanci subjektu kritické infrastruktury, kteří se podílejí na zajištění funkce prvku kritické infrastruktury, jsou za krizových stavů osvobozeni od pracovní povinnosti a pracovní výpomoci. Stejně jako ve výše uvedeném případě ani v tomto případě ale není osvobození od takovýchto povinností uplatnitelné pro všechny zaměstnance napříč organizací.

V případě subjektu kritické informační infrastruktury se tak bude jednat pouze o ty zaměstnance, kteří se podílejí na zajištění funkce prvku kritické informační infrastruktury, tedy zejména administrátory ve smyslu § 2 písm. a) vyhlášky o kybernetické bezpečnosti a některé další zaměstnance, s jejichž identifikací může i v tomto případě pomoci obsah evidence aktiv, kterou subjekt kritické informační infrastruktury vede podle § 4 vyhlášky o kybernetické bezpečnosti. Tímto postupem lze pak zajistit, že od pracovní povinnosti budou osvobozeni jen ti zaměstnanci, kteří jsou skutečně klíčoví pro funkčnost aktiv vitálních pro funkci prvku kritické informační infrastruktury.

4 Povinnosti subjektů kritické infrastruktury z krizového zákona

Na druhou stranu je subjekt kritické infrastruktury povinen:

- **oznámit Úřadu** bez zbytečného odkladu **informace** o organizační, výrobní nebo jiné **změně**, je-li zřejmé, že tato změna může mít vliv na určení prvku kritické infrastruktury,[4]
- **vypracovat plán krizové připravenosti** subjektu kritické infrastruktury, a to do jednoho roku ode dne nabytí právní moci opatření obecné povahy, kterým byl subjekt určen subjektem kritické infrastruktury,[5] a umožnit Úřadu vykonání kontroly tohoto plánu,[6]

  a

- **určit styčného bezpečnostního zaměstnance a jeho určení oznámit Úřadu,** a to bez zbytečného odkladu.[7]

4.1 Oznámení změn, které mohou mít vliv na určení prvku kritické infrastruktury

Pokud u subjektu kritické infrastruktury dojde k organizační, výrobní nebo jiné změně a je-li zřejmé, že tato změna může mít vliv na určení prvku kritické infrastruktury, zejména jde-li o trvalé zastavení provozu, ukončení činnosti, nebo restrukturalizaci, je jeho povinností o takové změně bez zbytečného odkladu informovat Úřad. Tato povinnost souvisí a navazuje na povinnost poskytnout informace nezbytné k určení prvku kritické infrastruktury a povinnost poskytnout další součinnost při ochraně kritické infrastruktury v souladu s § 29 odst. 7 krizového zákona.

V případě prvku kritické informační infrastruktury se tak bude jednat především o ukončení užívání určeného systému, změnu účelu jeho používání apod.

Oznámení změn nemá stanoven žádný závazný formát a je možné jej učinit prostřednictvím e-mailové adresy elektronické podatelny na posta@nukib.cz nebo prostřednictví datové schránky Úřadu: zzfnkp3. Samozřejmostí je, že z takového oznámení bude možné zjistit kdo jej činí, čeho se týká a co je podstatou oznámené změny.

4.2 Plán krizové připravenosti

Pojem „plán krizové připravenosti“ se v krizovém zákoně používá jako souhrnný pojem pro plán, který právnické a podnikající fyzické osoby zpracovávají za účelem plnění povinností z krizového zákona. Prakticky je však potřeba mít na paměti, že podle krizového zákona existují *de facto* dva druhy plánů krizové připravenosti.

1) **Plán krizové připravenosti podle § 29 odst. 1 krizového zákona**
   Plán, který jakékoliv právnické a podnikající fyzické osoby připravují z toho důvodu, že jim byla v rámci krizových plánů krajů nebo ministerstev, ústředních správních úřadů (mezi nimi také např. Úřad) a případně dalších orgánů krizového řízení uložena určitá povinnost

[4] § 29a písm. c) krizového zákona
[5] § 29b krizového zákona
[6] § 29a písm. b) krizového zákona
[7] § 29c odst. 1 krizového zákona

k řešení krizových situací.

Tento typ plánu krizové připravenosti není předmětem tohoto dokumentu. V případě nutnosti vypracovat tento plán krizové připravenosti doporučujeme obrátit se na orgán krizového řízení, který subjekt do svého krizového plánu zahrnul.

2) **Plán krizové připravenosti subjektu kritické infrastruktury podle § 29b krizového zákona**
Plán, v rámci kterého subjekt kritické infrastruktury identifikuje možná ohrožení funkce prvku kritické infrastruktury a stanoví opatření na jeho ochranu. Bude se jednat o opatření organizačního, administrativního, technického a jiného rázu, ať již činěná vlastními silami a prostředky subjektu kritické infrastruktury, nebo za pomoci jiných subjektů, orgánů a složek. Plán krizové připravenosti zpracuje subjekt kritické infrastruktury do jednoho roku od určení prvku kritické infrastruktury.

Tomuto typu plánu krizové připravenosti se tento dokument dále věnuje a uvádí bližší detaily jeho zpracování z pohledu kritické informační infrastruktury.

Zpracování obou typů plánů krizové připravenosti se řídí *„Metodikou zpracování plánů krizové připravenosti podle § 17 až 18 nařízení vlády č. 462/2000 Sb.“* (dále jen „Metodika“) vydanou Hasičským záchranným sborem České republiky[8], avšak níže v tomto dokumentu jsou pro plán krizové připravenosti subjektu kritické infrastruktury uvedena některá specifika.

Plán krizové připravenosti subjektu kritické infrastruktury se skládá ze základní, operativní a pomocné části – konkrétní náležitosti a způsob zpracování plánu krizové připravenosti obsahuje nařízení vlády č. 462/2000 Sb.

Základní část obsahuje:

- vymezení předmětu činnosti subjektu kritické infrastruktury a opatření, která byla důvodem zpracování plánu krizové připravenosti,
- charakteristiku krizového řízení,
- přehled a hodnocení možných zdrojů rizik a analýzy ohrožení a jejich možný dopad na činnost subjektu kritické infrastruktury,
- seznam prvků kritické infrastruktury a
- identifikaci možných ohrožení funkce prvku kritické infrastruktury.

Operativní část obsahuje:

- přehled opatření vyplývajících z krizového plánu příslušného orgánu krizového řízení a způsob zajištění jejich provedení,
- způsob zabezpečení akceschopnosti subjektu kritické infrastruktury pro zajištění provedení krizových opatření a ochrany činnosti subjektu kritické infrastruktury,

[8] Dostupné zde: https://www.hzscr.cz/clanek/dokumenty-ke-stazeni.aspx

- postupy řešení krizových situací identifikovaných v analýze ohrožení,
- plán opatření hospodářské mobilizace, pokud je subjekt kritické infrastruktury dodavatelem mobilizační dodávky,
- přehled spojení na příslušné orgány krizového řízení a
- přehled plánů zpracovávaných podle zvláštních právních předpisů využitelných při řešení krizových situací (plány povodňové, pandemické, epidemiologické atd.).

Tyto náležitosti musí být uzpůsobeny tak, aby se týkaly ochrany funkce prvku kritické informační infrastruktury. Proto musí obsahovat i opatření na ochranu funkce prvku kritické informační infrastruktury.

Pomocná část obsahuje:

- přehled právních předpisů využitelných při přípravě na krizové situace a jejich řešení,
- přehled uzavřených smluv k zajištění provedení opatření, která byla důvodem zpracování plánu krizové připravenosti,
- zásady manipulace s plánem krizové připravenosti,
- geografické podklady a
- další dokumenty související s připraveností na krizové situace a jejich řešením.

Rovněž tyto náležitosti musí být zaměřeny na ochranu funkce prvku kritické informační infrastruktury.

Pokud subjekt kritické infrastruktury provozuje více částí jednoho prvku kritické infrastruktury, může pro každou takovou část zpracovat dílčí plán krizové připravenosti. Tyto dílčí plány tvoří součást plánu krizové připravenosti subjektu kritické infrastruktury.

Subjekt kritické infrastruktury při přípravě plánu krizové připravenosti ve vlastním zájmu spolupracuje s orgánem krizového řízení, který zpracovává krizový plán (v případě kritické informační infrastruktury se jedná o Úřad). Součinností se subjekt kritické infrastruktury může vyhnout případným nedostatkům v plánu krizové připravenosti, na jejichž existenci by upozornil orgán krizového řízení při následné kontrole. Projednáno je zejména zaměření a rozsah plánu, podíl a rozsah spolupráce s dalšími subjekty, termíny pro průběžnou kontrolu prací včetně závěrečného termínu zpracování plánu, a způsob manipulace s plánem.[9]

Aktualizace plánu krizové připravenosti se provádí v čtyřletých cyklech od jeho schválení. Pokud dojde ke změně, mající dopad na obsah plánu, aktualizuje se bezodkladně.[10]

[9] § 18 odst. 2) nařízení vlády č. 462/2000 Sb.
[10] § 19 odst. 2) nařízení vlády č. 462/2000 Sb.

4.3 Plán krizové připravenosti v kontextu bezpečnostních opatření podle zákona o kybernetické bezpečnosti

V souvislosti s tím, že subjekt kritické informační infrastruktury musí plnit jak povinnosti z krizového zákona, tak povinnosti ze zákona o kybernetické bezpečnosti, nabízí se možnost **provázání obsahu plánu krizové připravenosti s požadavky, které jsou vyžadovány v rámci řízení kontinuity činností, resp. politiky řízení a plánu kontinuity činností** podle § 15, řízení rizik podle § 5 a dalších požadavků daných vyhláškou o kybernetické bezpečnosti, kdy se činnosti a dokumenty vyžadované oběma právními předpisy překrývají, či doplňují. Tuto možnost uznává i krizový zákon[11] a zákon o kybernetické bezpečnosti to samozřejmě nezakazuje.

Srovnání požadavků na tyto dva instituty je následující:

Požadavek plánu krizové připravenosti podle krizového zákona	Možný způsob splnění požadavku vycházející z Metodiky, avšak s ohledem na plnění bezpečnostních opatření podle zákona o kybernetické bezpečnosti
- vymezení předmětu činnosti subjektu kritické infrastruktury a opatření, která byla důvodem zpracování plánu krizové připravenosti	- informace, v rámci níž je uveden předmět činnosti, identifikační údaje subjektu a identifikace právního titulu určení kritické informační infrastruktury (opatření obecné povahy nebo usnesení vlády)
- charakteristika krizového řízení	- vymezení organizačních částí podílejících se na přípravě na krizové situace a jejich řešení, předpokládané změny organizační struktury nezbytné k zabezpečení činnosti za krizové situace a plnění opatření vyplývajících z krizového plánu, definování orgánů vytvořených a aktivovaných za účelem řešení krizové situace a zabezpečení plnění opatření vyplývajících z krizového plánu a vazby na příslušné orgány krizového řízení a krizové štáby, se kterými bude právnická nebo podnikající fyzická osoba spolupracovat při plnění opatření vyplývajících z krizového plánu - např. v rámci řízení kontinuity činností (politika řízení kontinuity činností)

[11] § 29b odst. 2 krizového zákona

- přehled a hodnocení možných zdrojů rizik a analýzy ohrožení a jejich možný dopad na činnost subjektu kritické infrastruktury	- výčet konkrétních hrozeb, které mohou způsobit vznik krizové situace a ohrozit plnění opatření vyplývajících z krizového plánu - např. v rámci procesu řízení rizik (hodnocení rizik), resp. řízení kontinuity činností
- seznam prvků kritické infrastruktury	- identifikace prvků kritické informační infrastruktury, jichž je subjekt správcem
- identifikace možných ohrožení funkce prvku kritické infrastruktury	- výčet možných ohrožení, které mohou narušit funkci prvku kritické infrastruktury - např. v rámci procesu řízení rizik (identifikace hrozeb a zranitelností), resp. řízení kontinuity činností
- přehled opatření vyplývajících z krizového plánu příslušného orgánu krizového řízení a způsob zajištění jejich provedení	- podrobný popis úkolů a opatření, které byly důvodem zpracování plánu krizové připravenosti, vymezení konkrétních postupů realizace úkolů a opatření, které byly důvodem zpracování plánu krizové připravenosti a definování předpokládaných požadavků na síly a prostředky pro realizaci úkolů a opatření, které byly důvodem zpracování plánu krizové připravenosti - např. v rámci řízení kontinuity činností (politika řízení kontinuity činností)
- způsob zabezpečení akceschopnosti subjektu kritické infrastruktury pro zajištění provedení krizových opatření a ochrany činnosti subjektu kritické infrastruktury	- popis systému fyzické ochrany se zaměřením na fyzickou ostrahu, technickou ochranu a režimová opatření, zabezpečení provedení změny organizační struktury právnické nebo podnikající fyzické osoby za krizové situace, zabezpečení způsobu komunikace organizačních částí za krizové situace a definování odpovědných osob včetně uvedení pravomocí a způsobu jejich aktivace při plnění opatření vyplývajících z krizového plánu za krizového situace - např. v rámci řízení kontinuity činností (politika řízení kontinuity činností)

- postupy řešení krizových situací identifikovaných v analýze ohrožení	- definování plánovaných opatření (včetně uvedení odpovědnosti za jejich provedení) realizovaných za účelem řešení krizové situace a předpokládané požadavky na síly a prostředky nezbytné k řešení krizové situace - např. v rámci řízení kontinuity činností (plány kontinuity činností)
- plán opatření hospodářské mobilizace, pokud je subjekt kritické infrastruktury dodavatelem mobilizační dodávky	- platí jen v případě dodavatelů mobilizační dodávky podle zákona č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy - provede se zpracováním plánu opatření hospodářské mobilizace podle § 2 odst. 1 písm. f) zákona o hospodářských opatřeních pro krizové stavy
- přehled spojení na příslušné orgány krizového řízení	- seznam telefonních kontaktů a elektronických adres na příslušné orgány krizového řízení a další subjekty podílející se na připravenosti na krizové situace a jejich řešení - např. v rámci řízení kontinuity činností (plány kontinuity činností)
- přehled plánů zpracovávaných podle zvláštních právních předpisů využitelných při řešení krizových situací (plány povodňové, pandemické, epidemiologické atd.)	- seznam dalších plánovacích dokumentů, které je možné využít při řešení krizové situace - např. v rámci řízení kontinuity činností (plány kontinuity činností)
- přehled právních předpisů využitelných při přípravě na krizové situace a jejich řešení	- výčet předpisů využitelných při přípravě na krizové situace a jejich řešení, které mohou ohrozit plnění opatření vyplývajících z krizového plánu a při realizaci plnění opatření vyplývajících z krizového plánu za krizové situace - např. v rámci řízení kontinuity činností (politika řízení kontinuity činností)
- přehled uzavřených smluv k zajištění provedení opatření, která byla důvodem zpracování plánu krizové připravenosti	- přehled smluv a dokumentů, uzavřených k zajištění provedení opatření, které byly důvodem zpracování plánu krizové připravenosti zejména za účelem poskytnutí pomoci, spolupráce nebo dodávky služby - např. v rámci řízení kontinuity činností (plány kontinuity činností) nebo řízení dodavatelů (evidence dodavatelů)

- zásady manipulace s plánem krizové připravenosti	- informace obsahující zejména místo uložení, způsob aktualizace a stanovení pravidel manipulace s plánem krizové připravenosti, seznam organizačních částí odpovědných za zpracování jednotlivých částí plánu krizové připravenosti a další informace (zda je některá z částí plánu krizové připravenosti označena jako obchodní tajemství, utajovaná informace nebo zvláštní skutečnosti) - např. v rámci řízení kontinuity činností (politika řízení kontinuity činností)
- geografické podklady a další dokumenty související s připraveností na krizové situace a jejich řešením	- geografické podklady využívané při přípravě na krizové situace a jejich řešení, které mohou ohrozit plnění opatření vyplývajících z krizového plánu a při realizaci plnění opatření vyplývajících z krizového plánu za krizové situace v analogové nebo digitální formě - např. v rámci řízení kontinuity činností (plány kontinuity činností)

Jak je z výše uvedeného patrné, většina požadavků na obsah plánu krizové připravenosti subjektu kritické infrastruktury má svůj odraz v procesu řízení kontinuity činností podle vyhlášky o kybernetické bezpečnosti.

Pro úplnost je vhodné uvést, že požadavky procesu řízení kontinuity činností podle vyhlášky o kybernetické bezpečnosti spočívají v následujícím:

- stanovení práv a povinnosti administrátorů a osob zastávajících bezpečnostní role,
- hodnocení a dokumentace možných dopadů kybernetických bezpečnostních incidentů pomocí hodnocení rizik a analýzy dopadů,
- posouzení možných rizik souvisejících s ohrožením kontinuity činností,
- stanovení cílů řízení kontinuity činností formou určení
    - minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu kritické informační infrastruktury,
    - doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb kritické informační infrastruktury,
    - bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání,

- vypracování, aktualizace a pravidelné testování potřebných plánů kontinuity a havarijních plánů souvisejících s provozováním kritické informační infrastruktury a souvisejících služeb,
- postupy pro realizaci opatření vydaných Úřadem.

Jak je patrné, subjekt kritické informační infrastruktury může sloučit výše uvedené výčty požadavků a zpracovat je v rámci jednoho společného dokumentu. Hlavním smyslem všech těchto požadavků je to, aby subjekt získal lepší představu o potřebných krocích v případě krize a tyto dokumentu mu v tom co nejvíce pomohly.

Úřad má v souladu s § 9 odst. 3 písm. e) krizového zákona pravomoc kontrolovat plán krizové připravenosti subjektů kritické informační infrastruktury, stejně tak jako má podle § 23 zákona o kybernetické bezpečnosti pravomoc kontrolovat proces řízení kontinuity činností. Také z tohoto důvodu nepovažuje za nutné vést tyto dokumenty odděleně jako dva separátní dokumenty. Je také vhodné vzít v potaz, že absence plánu krizové připravenosti u subjektu kritické infrastruktury není krizovým zákonem klasifikována jako přestupek. Na druhou stranu je však potřeba také vědět, že řízení kontinuity činností je bezpečnostním opatřením podle zákona o kybernetické bezpečnosti a jako takové může být v případě nedostatků Úřadem sankcionováno až do výše 5 000 000 Kč.[12]

4.4 Styčný bezpečnostní zaměstnanec

Úkolem styčného bezpečnostního zaměstnance je poskytovat jménem subjektu kritické infrastruktury součinnost při plnění úkolů podle krizového zákona. Pro doplnění je možné uvést, že role styčného bezpečnostního zaměstnance je převzata ze směrnice Rady 2008/114/ES, která hovoří o styčných bezpečnostních úřednících a uvádí k nim, že *„(…) by měl být jmenován styčný bezpečnostní úředník s cílem usnadnit spolupráci a komunikaci s vnitrostátními orgány příslušnými pro ochranu kritické infrastruktury“.*

V souvislosti se svými úkoly proto styčný bezpečnostní zaměstnanec poskytuje součinnost Úřadu při výkonu kontroly plánu krizové připravenosti a ochrany prvku kritické infrastruktury, podílí se na zpracování plánu krizové připravenosti a jeho aktualizaci, oznamuje Úřadu informace ohledně změn majících vliv na určení prvku kritické infrastruktury a z povahy věci plní další úkoly, které s ochranou a bezpečností prvku kritické infrastruktury souvisejí.

Krizový zákon také upravuje situaci, kdy nebyl styčný bezpečnostní zaměstnanec dosud určen – v takovém případě jeho úkoly plní přímo subjekt kritické infrastruktury.

Krizový zákon dále upravuje požadavky, které jsou na styčného bezpečnostního zaměstnance kladeny. Podle krizového zákona musí splňovat odborné vzdělání (kvalifikaci), které bude garantovat řádný výkon jeho činností – podmínkou je vysokoškolské vzdělání ve studijním oboru, který je komplexně zaměřen na oblast zajišťování bezpečnosti České republiky ochranu

[12] § 25 odst. 3 písm. b) zákona o kybernetické bezpečnosti

obyvatelstva nebo na krizové řízení.[13]. Tuto podmínku lze nahradit tím, že osoba, která má plnit úkoly styčného bezpečnostního zaměstnance, alespoň 3 roky aktivně působila v oblasti zajišťování bezpečnosti České republiky, ochrany obyvatelstva nebo krizového řízení.

4.5 Styčný bezpečnostní zaměstnanec v kontextu bezpečnostních opatření podle zákona o kybernetické bezpečnosti

V prvé řadě je potřeba uvést, že role styčného bezpečnostního zaměstnance se nevylučuje s bezpečnostními rolemi dle § 7 vyhlášky o kybernetické bezpečnosti, naopak, **náplň jeho činnosti se shoduje s požadavky kladenými na činnost manažera kybernetické bezpečnosti.** Také jeho odpovědností je plnění úkolů spojených s řízením bezpečnosti informací a součinnost s Úřadem.

V praxi tak není s plněním povinnosti určit styčného bezpečnostního zaměstnance u subjektů kritické informační infrastruktury žádný problém, a to také z toho důvodu, že pokud není jmenován (např. u menších subjektů nemusí být k dispozici zaměstnanec disponující požadovanou kvalifikací), plní jeho činnosti sám subjekt kritické infrastruktury. Z tohoto důvodu také není absence styčného bezpečnostního zaměstnance krizovým zákonem sankcionována.

[13] Tyto studijní obory musí být akreditované Národním akreditačním úřadem v souladu se zákonem č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon).

5 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách Národní úřad pro kybernetickou a informační bezpečnost - Doporučení k používání protokolu TLP ke sdílení chráněných informací (nukib.cz)). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená TLP: RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová TLP: AMBER	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám, než výše uvedeným, nesmí být informace poskytnuta. Původce informace může rozsah sdílení dále omezit.
Zelená TLP: GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá TLP: (WHITE)	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
29. listopadu 2021	1.0	OREG	Vytvoření dokumentu
22. prosince 2022	1.1	OREG	Změna kontaktních údajů