Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č.J. NEPŘIŘAZENO • BRNO • 26. BŘEZNA 2021

VERZE DOKUMENTU: 1.0

# PRAVIDLA URČOVÁNÍ A OVĚŘENÍ AKTUÁLNOSTI URČENÍ KRITICKÉ INFORMAČNÍ INFRASTRUKTURY

# Obsah

# 1 Úvod

Tento dokument seznamuje s pravidly určování kritické informační infrastruktury, tedy prvku/prvků kritické infrastruktury v odvětví VI. Komunikační a informační systémy, oblasti G. Kybernetické bezpečnosti nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury (dále jen „nařízení vlády“).

**Kritickou informační infrastrukturou** se rozumí prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti.[1]

**Určování kritické informační infrastruktury** provádí Národní úřad pro kybernetickou a informační bezpečnosti (dále jen „Úřad“) na základě zmocnění v § 22 písm. m) a n) zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „zákon o kybernetické bezpečnosti“), a na základě § 9 odst. 3 písm. c) zákona č. 240/2000 Sb., o krizovém řízení (dále jen „krizový zákon“), a nařízení vlády.

Zákon o kybernetické bezpečnosti ukládá v § 22 písm. o) Úřadu povinnost **ověřovat každé 2 roky aktuálnost určení prvků kritické infrastruktury** určených v odvětví VI. Komunikační a informační systémy, oblasti G. Kybernetické bezpečnosti nařízení vlády.

Proces ověření aktuálnosti určení kritické informační infrastruktury vychází z procesu určování kritické informační infrastruktury.

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

**Národní úřad pro kybernetickou a informační bezpečnost**

Mučednická 1125/31

616 00 Brno – Žabovřesky

Tel.: +420 541 110 560

E-mail: regulace@nukib.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje samotný proces určování, 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.

[1] § 2 písm. b) zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve spojení s § 2 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

# 2 Pravidla určování a ověřování aktuálnosti určení kritické informační infrastruktury

Zákon o kybernetické bezpečnosti ukládá v § 22 písm. m) a n) Úřadu povinnost zasílat podle krizového zákona Ministerstvu vnitra návrh prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, jejichž provozovatelem je organizační složka státu, anebo **určovat podle krizového zákona prvky kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti v případě, že se nejedná o organizační složku státu.**

Zákon o kybernetické bezpečnosti Úřadu rovněž ukládá v § 22 písm. o) povinnost **ověřovat každé 2 roky aktuálnost určení prvků kritické infrastruktury** určených v odvětví VI. Komunikační a informační systémy, oblasti G. Kybernetické bezpečnosti nařízení vlády.

## 2.1 Posuzovaný informační systém

Nejdříve je důležité definovat, co je to informační systém. **Informační systém je jako pojem v zákoně o kybernetické bezpečnosti vždy vymezen službou, pro kterou existuje.[2] A jako takový je tvořen vždy aktivy – tedy jak technickým a programovým vybavením a komunikačními prostředky, tak také objekty, zaměstnanci a dodavateli, stejně jako informacemi, které systém zpracovává, a službami (procesy), které systém poskytuje – na jejichž fungování je závislé poskytování předmětné služby. Jedná se tedy o aktiva, která přímo podporují výkon předmětné služby v daném rozsahu a kvalitě.**

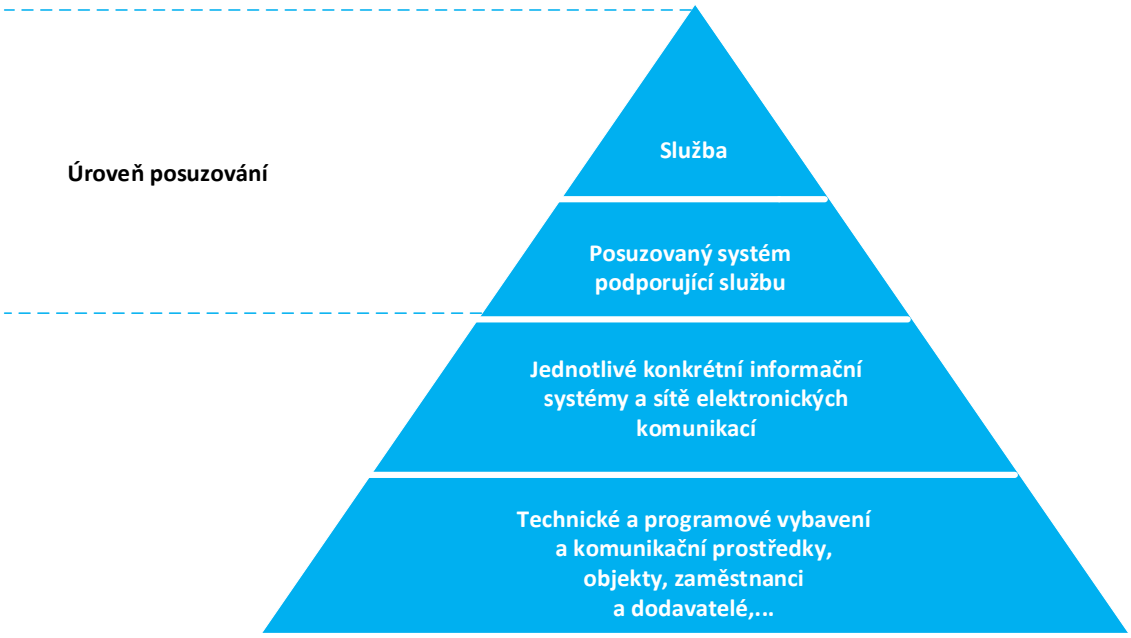
Pokud je pro poskytování celého rozsahu předmětné služby používáno více informačních systémů v užším slova smyslu (např. specializované systémy, samostatné programové prostředky a aplikace apod., spolu se souvisejícími technickými a personálními prostředky), všechny tyto „subsystémy“ tvoří v souhrnu jeden informační systém, tedy celek, u kterého je dále posuzováno, zda naplňuje průřezová a odvětvová kritéria nařízení vlády.

**Pro účely tohoto dokumentu v návaznosti na proces určování nebo ověření aktuálnosti určení kritické informační infrastruktury bude výše popsaný informační systém (jak jej chápe zákon o kybernetické bezpečnosti) označován dále také jako „posuzovaný systém“, aby nedocházelo k nedorozumění při výkladu těchto pojmů.**

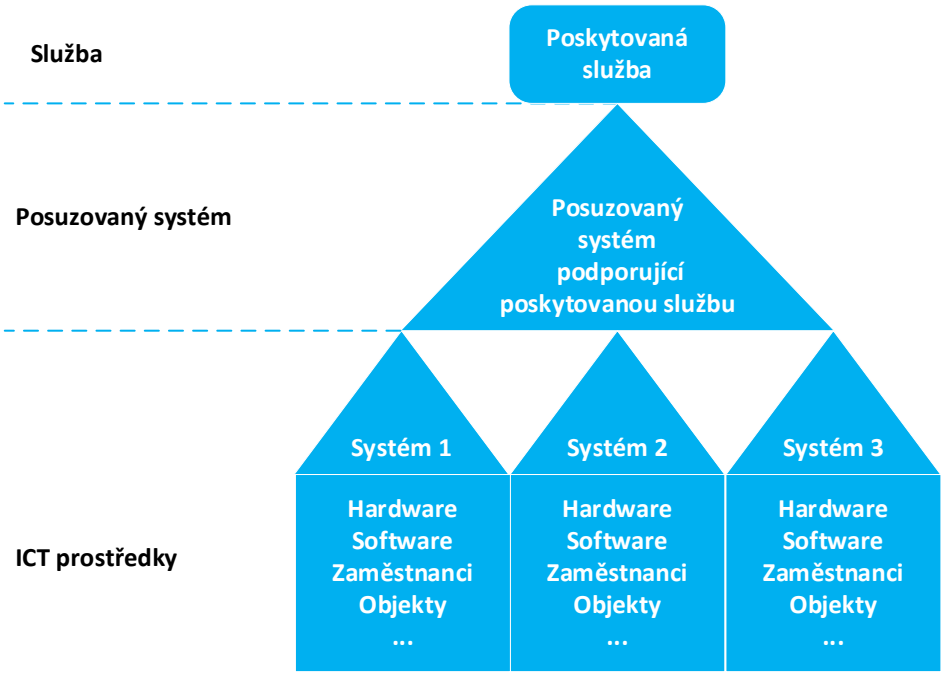
**Pokud je předmětem posuzování komunikační systém, platí pro jeho určení jako kritické informační infrastruktury stejná pravidla jako pro informační systém.**

Výše uvedené znázorňují také následující obrázky č. 1 a 2.

[2] Tj. organizace si nepořizují, nevyvíjejí a neudržují systémy jen tak – systém má organizace vždy za určitým účelem, aby poskytoval organizaci určitou službu. Je tomu tak vždy, nehledě na to, zda je to služba pro interní nebo externí potřeby organizace.




Obrázek č. 1: Úroveň posuzování informačního systému




Obrázek č. 2: Informační systém z pohledu poskytované služby

## 2.3 Hodnocení průřezových kritérií

**Posuzuje se narušení bezpečnosti informací (kybernetický bezpečnostní incident) z pohledu tří bezpečnostních domén (dostupnost, důvěrnost a integrita).**

**Bere se v úvahu nejhorší možný scénář** (např. výpadek výroby tepla v zimě namísto v létě; výpadek nemocničního systému během krize; kompromitace celého systému, nejen jeho části atd.).

Při hodnocení průřezových kritérií **se neuvažují bezpečnostní opatření, která má organizace zavedena**[3] za účelem zajištění toho, aby k narušení bezpečnosti informací nemohlo dojít (nebo s jen minimální pravděpodobností). Tato opatření jsou zavedena právě z důvodu určité významnosti informačního systému a je potřeba mít na paměti, že bezpečnostní opatření (nejde-li o samotnou architekturu systému nebo takové provedení opatření, které není možné žádným způsobem obejít) obvykle sama o sobě neeliminují riziko incidentu v systému zcela a mohou či nemusí fungovat tak, jak správce systému předpokládá. Proces určování kritické informační infrastruktury (včetně ověření aktuálnosti určení kritické informační infrastruktury) je totiž postupem, kterým dochází ke zjištění úrovně významnosti tohoto systému, nikoliv k zjištění úrovně zabezpečení. Pokud by se k bezpečnostním opatřením přihlíželo, došlo by k zařazení systémů na základě úrovně jejich zabezpečení, nikoliv na základě úrovně jejich významnosti. Zároveň by takový přístup vedl k absurdní situaci, že by byly některé systémy zařazeny mezi kritickou informační infrastrukturu v době, kdy nebyly zabezpečeny, a důsledkem jejich zabezpečení by bylo jejich vyřazení z regulace. Pokud má organizace některá opatření zavedena, v případě určení již plní některé požadavky zákona o kybernetické bezpečnosti a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále také „vyhláška o kybernetické bezpečnosti“), nicméně to nemůže mít vliv na posouzení dopadů narušení bezpečnosti informací v systému.

**V rámci určování (včetně ověření aktuálnosti určení kritické informační infrastruktury) se provádí posouzení, zda existuje informační nebo komunikační systém, který naplňuje kritéria nařízení vlády.**

**Při posouzení dopadů narušení bezpečnosti informací na život a zdraví osob** se uvažují pouze ty mimořádné události, které by mohly nastat prostřednictvím posuzovaného systému. Ke stanovení maximálního možného počtu obětí (na životech i zdraví) lze podpůrně využít např. výpočty uvedené v havarijním plánu organizace. Uvažují se pouze primární dopady způsobené posuzovaným systémem.

[3] Pokud by byla bezpečnostní opatření brána v potaz, vedlo by to k paradoxní situaci, kdy by Úřad organizaci určil, protože ještě žádná bezpečnostní opatření zavedena nejsou, organizace by tato bezpečnostní opatření následně zavedla a v tu chvíli by přestala naplňovat dopadová kritéria. Proto při hodnocení dopadových kritérií odhlédněte od bezpečnostních opatření, která již máte zavedena.

**Pro účely výpočtu hospodářské ztráty** bude do hospodářské ztráty zahrnuto zejména následující:

- přímé škody na majetku nebo zdraví,
- hospodářská ztráta z přerušení činnosti, ušlý zisk,
- předpokládaná sankce (pokuta) v případě porušení norem, předpisů (upravujících ochranu osobních údajů, výkon činností úvěrových institucí aj.), smluv, včetně pokuty za znečištění životního prostředí,
- náklady na sanaci škod na životním prostředí,
- případné další specifické náklady.

Pokud je to možné, pro otázky dostupnosti se využije **metoda časových řezů** (např.: co by znamenalo narušení bezpečnosti informací informačního systému po dobu 1 hodiny, půl dne, 1 dne, 1 týdne a déle, je však potřeba držet se reálných scénářů, tedy nemá smysl uvažovat o tom, jaký byl dopad, pokud by informační systém byl nedostupný 10 let). Dále je třeba zvážit, jaké následky toto narušení bude mít na poskytování služby a jaká hospodářská ztráta tímto může být způsobena. V případě důvěrnosti a integrity nehrají časové řezy roli, k naplnění nejhoršího scénáře může dojít okamžitě. **Hospodářskou ztrátu způsobenou narušením bezpečnosti informací v posuzovaném systému je potřeba hodnotit v souhrnu**, tzn. všechny výše uvedené oblasti možné ztráty je nutno sčítat, stejně tak i pokud by **ztráta spojená s narušením dostupnosti, důvěrnosti nebo integrity informací v posuzovaném systému samostatně nedosahovala hodnoty 0,5 % HDP**, je třeba hodnotit dopadové kritérium jako naplněné, pokud by bylo minimální požadované hodnoty ztráty dosaženo alespoň v souhrnu.

Při posuzování naplnění dopadu narušení bezpečnosti informací posuzovaného systému na veřejnost se zvažuje, jaký dopad bude mít toto narušení na poskytovanou službu, kolika osob (zákazníků) se výpadek poskytování služby dotkne.

Při posuzovaní **dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob** lze vyjít např. z celkového počtu zákazníků, kterým je služba poskytována.

**Při určování (včetně ověření aktuálnosti určení) kritické informační infrastruktury Úřad nestanovuje rozsah sytému řízení bezpečnosti informací** (dále jen „rozsah ISMS“), ten si určuje organizace sama na základě povinností uvedených ve vyhlášce o kybernetické bezpečnosti. Vyhláška o kybernetické bezpečnosti jako jednu z prvních povinností definuje povinnost stanovit si rozsah ISMS. Navíc je to právě samotná organizace, která zná svůj systém nejlépe a je schopna posoudit všechny relevantní skutečnosti.

# 3 Proces určování a ověřování aktuálnosti určení kritické informační infrastruktury

Pokud při určování nebo ověření aktuálnosti určení kritické informační infrastruktury Úřad zjistí, že:

- došlo ke vzniku nové kritické informační infrastruktury,
- posuzovaný systém určený jako kritická informační infrastruktura nadále neplní kritéria stanovená nařízením vlády, nebo
- došlo ke změně posuzovaného systému a je třeba provést změnu určení,

vydá Úřad opatření obecné povahy (dále jen „OOP“), kterým zařadí nový prvek nebo změní stávající, nebo navrhne zařazení či změnu posuzovaného systému Ministerstvu vnitra (pokud se jedná o organizační složku státu).

## 3.1 Forma určování a ověřování aktuálnosti určení kritické informační infrastruktury

**Opatření obecné povahy**

Náležitosti řízení o vydání nového OOP jsou stanoveny zákonem č. 500/2004 Sb., správního řádu. V případech změny kritické informační infrastruktury se proces vydání OOP v zásadě neliší od procesu, kterým byla určena původní kritická informační infrastruktura.

Pokud při určování kritické informační infrastruktury Úřad zjistí, že posuzovaný systém naplňuje kritéria stanovená nařízením vlády, a jedná-li se o orgán nebo osobu, které nejsou organizační složkou státu, vydá OOP, kterým určí kritickou informační infrastrukturu.

Pokud při ověřování aktuálnosti určení kritické informační infrastruktury Úřad zjistí, že posuzovaný systém nadále nenaplňuje kritéria nařízení vlády nebo že se změnilo aktuální uspořádání kritické informační infrastruktury, vydá Úřad OOP, kterým zruší určení kritické informační infrastruktury nebo kterým změní určení kritické informační infrastruktury.

V případě, že novým OOP bude rozšířeno dosavadní určení, poběží v této nově určené části organizaci nová lhůta pro plnění povinností vyplývajících ze zákona o kybernetické bezpečnosti.

Proces určení nebo změny kritické informační infrastruktury trvá, i s ohledem na zákonem stanovené lhůty, tři až čtyři měsíce, ve složitějších případech i déle.

**Návrh prvků kritické infrastruktury**

Pokud je posuzovaný systém spravován organizační složkou státu, v případě, že Úřad zjistí, že vznikl nový systém, posuzovaný systém již neodpovídá určení, tedy změnilo se jeho uspořádání, nebo došlo k jeho zániku, navrhne Úřad tuto změnu Ministerstvu vnitra. Tento návrh je následně předložen vládě České republiky. Vláda České republiky rozhodne usnesením a navrhovaný informační systém určí v příloze k tomuto usnesení prvkem kritické infrastruktury, případně jeho určení zruší.

## 3.2 Fáze procesu určování a ověřování aktuálnosti určení kritické informační infrastruktury

Proces určování i ověřování aktuálnosti určení kritické informační infrastruktury má několik fází:

1. navázání kontaktu s organizací,
2. zajištění podkladů k určování nebo ověření aktuálnosti určení kritické informační infrastruktury,
3. posouzení naplnění kritérií nařízení vlády posuzovaným systémem,
4. ukončení řízení:
    a. pokud posuzovaný systém kritéria nařízení vlády splňuje:
        i. vydá Úřad OOP, čímž se určí nová, dosud neurčená kritická informační infrastruktura, nebo se jím změní aktuální uspořádání kritické informační infrastruktury,
        ii. navrhne Úřad prvky kritické infrastruktury, jejichž provozovatelem je organizační složka státu, a tento návrh zašle Ministerstvu vnitra, čímž se určí nová, dosud neurčená kritická informační infrastruktura, nebo se jím změní aktuální uspořádání kritické informační infrastruktury, nebo
        iii. Úřad v rámci ověření aktuálnosti určení kritické informační infrastruktury zjistí, že prvek kritické infrastruktury i nadále naplňuje kritéria nařízení vlády a není třeba jeho určení měnit, a řízení se ukončí.
    b. pokud posuzovaný systém kritéria nařízení vlády nenaplňuje, řízení o určení nové kritické informační infrastruktury se ukončí, nebo v případě ověření aktuálnosti určení kritické informační infrastruktury:
        i. vydá Úřad OOP, kterým určení kritické informační infrastruktury zruší,
        ii. navrhne Úřad prvky kritické infrastruktury, jejichž provozovatelem je organizační složka státu, ke zrušení a tento návrh zašle Ministerstvu vnitra.

# 4 Seznam použitých zkratek a pojmů

| | |
|---|---|
| **posuzovaný systém** | informační nebo komunikační systém, který je předmětem určování či ověřování aktuálnosti určení kritické informační infrastruktury |
| **rozsah ISMS** | rozsah sytému řízení bezpečnosti informací |
| **OOP** | opatření obecné povahy |
| **nařízení vlády** | nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury |
| **krizový zákon** | zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů |
| **zákon o kybernetické bezpečnosti** | zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů |
| **vyhláška o kybernetické bezpečnosti** | vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat |
| **Úřad** | Národní úřad pro kybernetickou a informační bezpečnost |

# 5 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách www.nukib.cz/cs/infoservis/doporuceni/1593-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci/). 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<br>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<br>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<br>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<br>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** |
| 26. března 2021 | 1.0 | Odbor regulace | Vytvoření dokumentu |