Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

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

VERZE DOKUMENTU: 1.0

CO SI PŘIPRAVIT NA PRVNÍ JEDNÁNÍ

Určování kritické informační infrastruktury

1 Úvod

Tento dokument má za cíl poskytnout informace o tom, co si připravit na první jednání s Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „Úřad“) k 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“).

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

Tel.: +420 541 110 560

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 Co si připravit

Hlavní náplní prvního společného jednání je posouzení informačních systémů či sítí elektronických komunikací, které jsou ve správě potenciálního povinného subjektu, zda naplňují kritéria nařízení vlády pro určení kritickou informační infrastrukturou. V této souvislosti a v zájmu hladkého průběhu osobních schůzek Úřad doporučuje mít na jednání připraveny informace či písemné podklady k následujícím níže uvedeným bodům (především tučně vyznačeným):

- **Činnosti a služby, které organizace zajišťuje.**
- **Přibližný počet (kvalifikovaný odhad) osob (právnických a fyzických), kterým je služba organizací poskytována.**
- **Procesy související se zajištěním služby.**
- **Seznam informačních systémů, které podporují nebo zajišťují činnosti podle předchozích bodů (dále jen „posuzovaný systém“).**
- **Jaké skupiny osob posuzovaný systém využívají (interní i externí) a jakým způsobem [uživatelský přístup (zápis, čtení, provádění změn), administrátorský přístup (správa systému)].**
- **Základní funkcionality posuzovaného systému.**
- **Přehled možných dopadů v případě narušení bezpečnosti informací (narušení dostupnosti, důvěrnosti, integrity) v rámci posuzovaného systému.**
- Zhodnocení posuzovaného systému, zda může naplnit kritéria pro určení kritickou informační infrastrukturou podle nařízení vlády.
- Architektura posuzovaného systému.
- Relevantní bezpečnostní dokumentace k posuzovanému systému (např. bezpečnostní zprávu, vnější a vnitřní havarijní plán apod.) či další relevantní podklady k bezpečnosti informačních a komunikačních technologií, například analýzu dopadu (BIA).

3 Kdo by se měl účastnit jednání

Jednání o určování kritické informační infrastruktury zahajuje Úřad z moci úřední, řízení vedou pověření zaměstnanci odboru regulace. Jednání s Úřadem by se měly účastnit osoby se znalostmi o skutečnostech uvedených v kapitole 2. Typicky jimi jsou:

- **Osoba oprávněná jednat za organizaci (na základě zmocnění, pověření, zápisu ve veřejném rejstříku).**
- **Osoba obeznámená s poskytovanými službami organizace (produktový manažer).**
- **Osoba obeznámená s řízením bezpečnosti v organizaci (bezpečnostní manažer, manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti apod.).**
- **Osoba obeznámená se zajištěním kontinuity činností organizace (business continuity manažer).**
- **Osoba obeznámená s informačními a komunikačními technologiemi organizace (technický pracovník).**

Osobou oprávněnou jednat za organizaci je osoba, která disponuje zmocněním (obvykle třetí osoba), pověřením (zaměstnanec organizace), či je zapsána ve veřejném rejstříku (statutární orgán, jednatel).

4 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 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**
26. března 2021	1.0	Odbor regulace	Vytvoření dokumentu