PORTÁL NÚKIB

Průvodce zařazením do bezpečnostní úrovně

TLP:CLEAR

23. července 2026

Verze 1.0

Národní úřad pro kybernetickou a informační bezpečnost

Obsah

1 Co se dozvím v tomto dokumentu?

Tento podpůrný materiál poskytuje orgánům veřejné správy (dále také „OVS“) metodickou podporu pro zařazení informačního systému veřejné správy (dále také „ISVS“), který si přejí provozovat prostřednictvím služeb cloud computingu, do odpovídající bezpečnostní úrovně dle vyhlášky č. 411/2025 Sb., o bezpečnostních úrovních informačních systémů veřejné správy (dále jen „vyhláška“). Podpůrný materiál je v zásadě použitelný také při určování bezpečnostní úrovně ISVS, nebo jejich komponent, dle vyhlášky č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy, kterou vydává Digitální a informační agentura, a to bez ohledu na způsob provozování hodnoceného systému. Tento materiál současně vysvětluje základní pojmy obsažené ve vyhlášce a poskytuje čtenáři stručný návod, jakým způsobem hodnotit naplnění úrovní dopadu v dílčích dopadových oblastech z hlediska dostupnosti, důvěrnosti i integrity.

Pokud máte jakékoliv další otázky, podívejte se na web nukib.gov.cz nebo v případě otázek týkajících se zákona o kybernetické bezpečnosti pak na portal.gov.cz. Pro případ přetrvávajících dotazů nám napište na regulace@nukib.gov.cz.

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 Manažerské shrnutí

- OVS hodnotí nejzávažnější možné dopady v jednotlivých dopadových oblastech v případě narušení dostupnosti, důvěrnosti i integrity posuzovaného ISVS.
- V případě, že je posuzována pouze ta část ISVS, jejíž provoz má být zajišťován pomocí cloud computingu, musí taktéž zhodnotit vztah této části ISVS k ISVS jako celku.
- Při hodnocení dopadů je třeba respektovat základní principy hodnocení dopadů, tedy:
  - Nezkoumat příčiny narušení bezpečnosti.
  - Identifikovat opravdu nejhorší možné scénáře.
  - Neřešit pravděpodobnost výskytu těchto scénářů.
  - Neuvažovat jakákoliv bezpečnostní opatření.
- Výstupem hodnotícího procesu je minimálně písemný záznam ve formě Formuláře hodnocení bezpečnostních úrovní, jehož vzor je dostupný na webových stránkách NÚKIB.
- Důležitou součástí záznamu hodnocení je odůvodnění závěrů o naplnění dílčích dopadových úrovní.
- Bezpečnostní úroveň ISVS, k zajištění jehož provozu má být využíván cloud computing, je shodná s nejvyšší úrovní dopadu, které posuzovaný ISVS dosáhne při hodnocení jednotlivých oblastí dopadu.
- Nejvyšší stanovená bezpečnostní úroveň ISVS jako celku musí být stanovena alespoň pro jednu část posuzovaného ISVS. Jinak řečeno, systém zařazený např. v bezpečnostní úrovni „vysoká“ nejde dekomponovat na části, které budou všechny spadat pouze do bezpečnostních úrovní „nízká“ nebo „střední“.

3 Zařazení do bezpečnostní úrovně

3.1 Co je posuzováno a zařazováno do bezpečnostní úrovně?

Předmětem zařazování do odpovídající bezpečnostní úrovně je ISVS jako celek, nebo jeho části, jež mohou být provozovány prostřednictvím cloud computingu.

3.2 Základní principy a informace k zařazování

Obecně je úkolem OVS vyhodnotit, jaké nejzávažnější dopady může mít případný kybernetický bezpečnostní incident na ISVS, a to v každé jednotlivé oblasti dopadu (viz jednotlivé sloupce tabulky v příloze vyhlášky).

OVS přitom musí uvažovat nejhorší možné dopady z hlediska narušení dostupnosti, důvěrnosti i integrity v rámci posuzovaného ISVS a vzít v potaz jeho povahu jako celku. V případě, že do bezpečnostní úrovně zařazuje pouze část ISVS, musí taktéž zhodnotit vztah této části k ISVS jako celku. Konkrétní postup je popsán na příkladu níže v podkapitole 3.3.

3.2.1 Základní principy hodnocení dopadů

V rámci hodnocení je důležité respektovat následující základní principy:

- **Nezkoumají se příčiny narušení bezpečnosti.**

Z hlediska určení nejhorších možných dopadů není důležité, proč nebo jakým způsobem ke kybernetickému bezpečnostnímu incidentu došlo, ať už by to bylo v důsledku zneužití zranitelnosti konkrétního řešení nebo chyby uživatele daného systému. Posuzované dopady mohou být v obou případech v zásadě srovnatelné.

- **Identifikují se nejhorší možné „kritické“ scénáře.**

OVS by měl vždy objektivně zhodnotit, jaký je opravdu nejhorší možný scénář a nepodcenit důležitost posuzovaného ISVS v rámci dané organizace. Pokud se například zamýšlí nad narušením důvěrnosti či integrity určité databáze osobních údajů, měl by brát v potaz kompromitaci všech údajů. V případě narušení dostupnosti je pak třeba uvažovat úplnou ztrátu dostupnosti veškerých dat atp. Rozhodná taktéž není skutečnost, že k incidentu takového rozsahu v minulosti dosud nedošlo.

- **Neurčuje se pravděpodobnost výskytu jednotlivých scénářů.**

Má-li být identifikován nejhorší možný scénář, bude se zpravidla jednat o scénář s menší pravděpodobností výskytu. Takový dopad však správce nemůže ignorovat s poukazem na to, že je jeho potenciální výskyt velmi málo pravděpodobný, což úzce souvisí s principem nezohledňování bezpečnostních opatření. Hodnocení pravděpodobnosti zneužití zranitelností systému a realizace hrozeb je prováděno toliko v hodnocení rizik dle vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, nebo při zajišťování minimální kybernetické bezpečnosti dle vyhlášky č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.

- **Neuvažují se existující bezpečnostní opatření.**

Stěžejním principem celého hodnotícího procesu je hodnocení inherentních rizik, tedy že OVS nesmí při hodnocení potenciálních dopadů brát v potaz jakákoliv bezpečnostní opatření a redukovat tak závažnost případných dopadů. Nelze tak argumentovat způsobem „Budeme mít zavedeno opatření ABC, proto nemůže k dopadu takové intenzity nikdy dojít.“. Hodnocení dopadů primárně reprezentuje hodnotu systému pro organizaci, nikoliv úroveň zabezpečení daného systému.

3.2.2 Metoda hodnocení dopadů

Vhodnou metodou hodnocení dopadů, a v důsledku důležitosti celého ISVS, je řízené interview s garantem daného ISVS a garantem procesu či služby, kterou ISVS podporuje. K rozhovoru lze případně přizvat i další specialisty (ICT oddělení, technická správa, bezpečnostní oddělení apod.), jejichž expertíza je pro proces hodnocení dopadů přínosná. Interview by mělo být vedeno analytikem, který je znalý metodiky a postupů kvalitativního a kvantitativního hodnocení dopadů.

3.2.3 Požadavky na výstupy hodnocení

Po zpracování výsledků interview je vhodné zaslat výstup z hodnocení garantovi k revizi a odsouhlasení provedeného hodnocení. Výstupem hodnotícího procesu je minimálně písemný záznam ve formě Formuláře hodnocení bezpečnostních úrovní, jehož vzor je dostupný na webových stránkách NÚKIB. Důležitou součástí záznamu hodnocení je odůvodnění závěrů o naplnění dílčích dopadových úrovní. Bez patřičné úvahy zachycené ve formě odůvodnění jsou závěry hodnocení nepřezkoumatelné a nesrozumitelné pro kohokoliv dalšího kromě samotného autora (resp. hodnotitele).

3.3 Postup zařazení posuzovaného ISVS do bezpečnostní úrovně

Požadavky na vyplnění hodnoticího formuláře lze nejlépe vysvětlit na konkrétním příkladu fiktivní Evidence žadatelů a uživatelů sociálních služeb. Každý posuzovaný systém bude samozřejmě specifický, nelze proto předvídat standardní hodnoty dopadů. Typově obdobné systémy, například systémy spisové služby, mohou mít velmi rozdílné dopady s ohledem na subjekt, který je spravuje (např. ústřední orgán státní správy oproti obci s 5000 obyvateli).

3.3.1 Část A: Údaje o orgánu veřejné správy

Tato část formuláře obsahuje pouze identifikační údaje OVS, který je správcem hodnoceného ISVS. Tuto část není třeba blíže rozebírat.

3.3.2 Část B: Identifikace ISVS, k zajištění jehož provozu má být využíván cloud computing

V následující části formuláře je třeba vyplnit základní údaje týkající se hodnoceného ISVS. Důležité je zejména rozlišení, zda je řešení pomocí cloud computingu plánováno pro ISVS jako celek, nebo jen pro jeho určitou vyčleněnou část (dílčí evidenci údajů, uživatelskou platformu, úložiště atp.). Pokud je posuzována pouze část ISVS, pak je třeba tuto část ISVS určitým způsobem definovat a popsat její vztah k ISVS jako celku.

B: Identifikace informačního systému veřejné správy, u kterého je stanovována bezpečnostní úroveň	
Označení systému:	Evidence žadatelů a uživatelů sociálních služeb
Je řešení pomocí cloud computingu plánováno pro informační systém veřejné správy jako pro celek?	*Ne, pouze pro část*

V případě, že je řešení pomocí cloud computingu plánováno jen pro část informačního systému veřejné správy, definujte ji z hlediska funkčních kategorií, architektury, provozního modelu a bezpečnosti:

V této části může být popsána informační, aplikační či technologická architektura hodnocené části ISVS, resp. vazba této části na zbytek ISVS, který není provozován prostřednictvím služeb cloud computingu.

Při dekompozici systému na dílčí části je třeba pamatovat na ustanovení § 4 odst. 3 vyhlášky, ze kterého vyplývá, že **alespoň jedna** z dekomponovaných částí systému, který je ISVS, k zajištění jehož provozu má být využíván cloud computing, musí mít shodnou bezpečnostní úroveň, jakou by měl ISVS jako celek. Jinak řečeno, ISVS zařazený v bezpečnostní úrovni „vysoká“ nejde dekomponovat na části, které budou spadat **pouze** do bezpečnostních úrovní „nízká“ nebo „střední“. Jedna z částí musí stále být v bezpečnostní úrovni „vysoká“.

3.3.3 Část C: Výsledná bezpečnostní úroveň

V této části je obsažen výsledek hodnocení dopadů, tedy výsledná nejvyšší úroveň dopadu zařazovaného ISVS nebo jeho části, která vzejde z části D formuláře. Nejvyšší úroveň dopadu pak určuje výslednou jedinou bezpečnostní úroveň posuzovaného ISVS, která může nabývat hodnot „nízká“, „střední“, „vysoká“, nebo „kritická“.

3.3.4 Část D: Zhodnocení bezpečnostní úrovně podle přílohy vyhlášky

Jde o stěžejní část formuláře, kde musí OVS zachytit hodnocení nejhorších možných dopadů v jednotlivých vyjmenovaných oblastech dopadu a tyto své závěry náležitě odůvodnit. Pouze OVS totiž disponuje relevantními informacemi pro zhodnocení inherentních rizik a zařazení daného ISVS do odpovídající bezpečnostní úrovně.

D: Zhodnocení bezpečnostní úrovně podle přílohy vyhlášky		
Oblast dopadu	**Nejvyšší dosažená úroveň dopadu v příslušné oblasti**	**Odůvodnění***
A. Bezpečnost nebo zdraví lidí	z pohledu narušení dostupnosti	Narušení dostupnosti, důvěrnosti či integrity Evidence žadatelů a uživatelů sociálních služeb (dále také "Evidence") nemůže přímo jakkoli způsobit zranění jednotlivce ani skupiny lidí. Evidence slouží pouze jako jmenný seznam osob, není zde tedy jakákoli možnost ohrožení jejich zdraví či bezpečnosti.
	NÍZKÁ	
	z pohledu narušení důvěrnosti	
	NÍZKÁ	
	z pohledu narušení integrity	
	NÍZKÁ	
B. Ochrana osobních údajů	z pohledu narušení dostupnosti	Narušení bezpečnosti informací v rámci Evidence může negativně ovlivnit posuzovaný ISVS, který naplňuje dvě

	NÍZKÁ	a více kritérií z druhé skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů. Konkrétně je naplněno kritérium a) a b) z druhé skupiny kritérií, jelikož jsou zpracovávány zvláštní kategorie osobních údajů uživatelů systému a tímto zpracováním bude určitě dotčeno více než 10000 subjektů údajů.
	z pohledu narušení důvěrnosti	
	VYSOKÁ	
	z pohledu narušení integrity	
	VYSOKÁ	
C. Trestní řízení a páchání trestné činnosti	z pohledu narušení dostupnosti	Narušení dostupnosti, důvěrnosti či integrity Evidence nemůže přímo jakkoli vytvořit podmínky pro páchání trestných činů přisvojení pravomoci úřadu, zneužití pravomoci úřední osoby nebo padělání a pozměnění veřejné listiny ani nemůže ztížit jejich vyšetřování.
	NÍZKÁ	
	z pohledu narušení důvěrnosti	
	NÍZKÁ	
	z pohledu narušení integrity	
	NÍZKÁ	
D. Veřejný pořádek	z pohledu narušení dostupnosti	Narušení dostupnosti, důvěrnosti či integrity Evidence nemůže přímo jakkoli zapříčinit hromadné nepokoje nebo jinak narušit veřejný pořádek. V případě narušení bezpečnosti informací v Evidenci nelze důvodně předpokládat vznik nepokojů či narušování veřejného pořádku ze strany evidovaných osob.
	NÍZKÁ	
	z pohledu narušení důvěrnosti	
	NÍZKÁ	
	z pohledu narušení integrity	
	NÍZKÁ	
E. Mezinárodní vztahy	z pohledu narušení dostupnosti	Narušení dostupnosti, důvěrnosti či integrity Evidence nemůže přímo jakkoli negativně ovlivnit obraz České republiky v zahraničí. Evidence postrádá jakoukoli vazbu na mezinárodní vztahy České republiky.
	NÍZKÁ	
	z pohledu narušení důvěrnosti	
	NÍZKÁ	
	z pohledu narušení integrity	
	NÍZKÁ	
F. Důvěryhodnost orgánu veřejné správy	z pohledu narušení dostupnosti	Narušení dostupnosti Evidence nemůže negativně ovlivnit vztahy s jinými částmi orgánu veřejné moci, jinými organizacemi nebo vztahy s veřejností, nebo může vztahy s nimi negativně ovlivnit, avšak negativní následky mohou být nejvýše lokální. V případě narušení důvěrnosti či integrity informací obsažených v Evidenci by negativní následky mohly být nejvýše regionální, což odpovídá "střední" dopadové úrovni. Konkrétně by toto negativní ovlivnění vztahů s jinými organizacemi a veřejností spočívalo ve ztrátě důvěry v zabezpečení citlivých údajů evidovaných uživatelů
	NÍZKÁ	
	z pohledu narušení důvěrnosti	
	STŘEDNÍ	
	z pohledu narušení integrity	
	STŘEDNÍ	

		a žadatelů po narušení jejich integrity či důvěrnosti v důsledku kybernetického bezpečnostního incidentu.
G. Finanční ztráty	z pohledu narušení dostupnosti	Běžné výdaje ročního rozpočtu Fiktivního kraje na rok 2026 činí 13581000000 Kč (13,58 mld. Kč); 1 % z této částky tak odpovídá 135,8 milionům Kč. Narušení dostupnosti, důvěrnosti či integrity Evidence nemůže ani nepřímo vést k finančním ztrátám, nebo může vést k finančním ztrátám menším než 1 % běžných výdajů ročního rozpočtu Fiktivního kraje. Obnova dat z této evidence z důvodu narušení jejich integrity, důvěrnosti nebo dostupnosti by si dle kvalifikovaných odhadů vyžádala finanční výdaje (ztráty) max. ve výši jednotek milionů Kč.
	NÍZKÁ	
	z pohledu narušení důvěrnosti	
	NÍZKÁ	
	z pohledu narušení integrity	
	NÍZKÁ	
H. Zajišťování služeb	z pohledu narušení dostupnosti	Průměrný počet uživatelů sociálních služeb a žadatelů o jejich poskytnutí činí za rok 2025 celkem 24849 osob. Průměrný meziroční nárůst počtu žadatelů a uživatelů se stabilně pohybuje do 5 %, v roce 2026 a dalších letech tak lze očekávat obdobný nárůst počtu uživatelů posuzovaného systému. Narušení dostupnosti, důvěrnosti či integrity Evidence žadatelů a uživatelů sociálních služeb tak může způsobit omezení, narušení nebo nedostupnost služeb pro více než 5000, nejvíce však 50000 osob.
	STŘEDNÍ	
	z pohledu narušení důvěrnosti	
	STŘEDNÍ	
	z pohledu narušení integrity	
	STŘEDNÍ	

Vyplněný hodnoticí formulář pak může vypadat dle příkladu výše. Odůvodnění je v tomto případě zpracováno stručně bez jakýchkoli rozsáhlejších úvah či odkazů na další podklady.

Z provedeného příkladného hodnocení vychází, že nejvyšší dopadové úrovně dosahuje hodnocená část ISVS v oblasti B. Ochrana osobních údajů, kde je dopadová úroveň „vysoká“, což znamená, že výsledná bezpečnostní úroveň ISVS bude taktéž „vysoká“. Tento závěr je třeba uvést do části C formuláře (viz výše).

V případě, že je řešení pomocí cloud computingu plánováno jen pro část ISVS (jako v uvedeném příkladu), je nezbytné popsat, jakým způsobem byl v rámci zhodnocení bezpečnostní úrovně zohledněn vztah této části systému k ISVS jako celku, což lze učinit například následovně:

V rámci zhodnocení bezpečnostní úrovně posuzované části ISVS bylo zvlášť přihlédnuto ke skutečnosti, že ISVS obsahuje osobní údaje uživatelů a žadatelů, které jsou následně využívány v rámci dalších procesů prováděných ISVS jako celkem.

Evidence je v podstatě databankou vstupů a údajů pro další procesy, které se odehrávají ve zbylých částech ISVS.

Narušení dostupnosti, důvěrnosti či integrity jakýchkoliv informací obsažených v Evidenci uživatelů a žadatelů o poskytnutí sociálních služeb tak může narušit fungování ISVS jako celku.

Závěrem dotazníku je třeba vyplnit datum, ze kterého bude patrné, kdy ke zhodnocení ISVS došlo. Za příslušný OVS pak hodnoticí formulář podepíše k tomu oprávněný zaměstnanec či jiná osoba,

která byla příslušným OVS pověřena k zařazení ISVS do odpovídající bezpečnostní úrovně. Jednou z příloh hodnoticího formuláře by měl být dokument prokazující oprávnění dané osoby k provedení hodnocení daného ISVS.

3.4 Využití výstupů hodnocení

Hodnoticí formulář je písemným záznamem o procesu stanovení bezpečnostní úrovně ISVS k zajištění jehož provozu má být využíván cloud computing dle § 4 odst. 5 vyhlášky, který dokládá splnění zákonné povinnosti vyplývající z § 6n písm. d) zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, tedy zařazení ISVS, k zajištění jehož provozu má být využíván cloud computing, do bezpečnostní úrovně.

Zjištěná bezpečnostní úroveň OVS vymezuje, které konkrétní produkty zapsané v katalogu cloud computingu může v rámci svého ISVS použít. Je-li posuzovaný ISVS zařazen např. do bezpečnostní úrovně „střední“, lze pro jeho provoz pořizovat služby cloud computingu zapsané v katalogu **minimálně** v bezpečnostní úrovni „střední“.

4 Zdroje a další materiály

- zákon č. 264/2025 Sb., o kybernetické bezpečnosti
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
- vyhláška č. 411/2025 Sb., o bezpečnostních úrovních informačních systémů veřejné správy
- vyhláška č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy
- Znalostní web odboru Hlavního architekta eGovernmentu ČR
- Národní architektonický plán
- Národní architektonický rámec
- Dekompozice informačních systémů [Architektura eGovernmentu ČR]

5 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
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.
TLP:AMBER+STRICT	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
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.
TLP:CLEAR	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**
23. července 2026	1.0	OREG	Vytvoření dokumentu