Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

BRNO • 5. LEDNA 2023 • VERZE DOKUMENTU: 1.1

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

PRŮVODCE ZAŘAZENÍM POPTÁVANÉHO CLOUD COMPUTINGU DO BEZPEČNOSTNÍ ÚROVNĚ

Podpůrný materiál

1 Úvod

Tento podpůrný materiál poskytuje orgánům veřejné moci metodickou podporu pro zařazení informačního nebo komunikačního systému, který si přejí provozovat prostřednictvím služeb cloud computingu, do odpovídající bezpečnostní úrovně dle vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci (dále jen „vyhláška“). Podpůrný materiál je v zásadě použitelný také při určování bezpečnostní úrovně informačních systémů veřejné správy, nebo jejich komponent, dle vyhlášky o dlouhodobém řízení informačních systémů veřejné správy, kterou vydává Ministerstvo vnitra ČR, a to bez ohledu na způsob provozování hodnoceného systému.

Orgánům veřejné moci jsou vysvětleny základní pojmy obsaženy ve vyhlášce a poskytnut stručný návod, jakým způsobem hodnotit naplnění úrovní dopadu v dílčích dopadových oblastech z hlediska dostupnosti, důvěrnosti i integrity.

V případě dotazů se prosím obracejte na sekretariát NÚKIB:

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 Manažerské shrnutí

- Poptávaným cloud computingem není konkrétní produkt poskytovatele, ale posuzovaný informační nebo komunikační systém nebo jeho část, jejichž správcem je orgán veřejné moci.
- Správce hodnotí **nejhorší možné dopady** v jednotlivých dopadových oblastech v případě narušení dostupnosti, důvěrnosti i integrity posuzovaného poptávaného cloud computingu.
- V případě, že je poptávaným cloud computingem pouze část systému musí taktéž zhodnotit **vztah této části k systému 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.[1]
- Důležitou součástí záznamu hodnocení je **odůvodnění závěrů** o naplnění dílčích dopadových úrovní.

> Bezpečnostní úroveň pro využívání poptávaného cloud computingu orgánem veřejné moci je shodná s nejvyšší úrovní dopadu, které poptávaný cloud computing dosáhne při hodnocení jednotlivých oblastí dopadu.

- **Významný informační systém** provozovaný jako celek prostřednictvím služeb cloud computingu spadá automaticky minimálně do bezpečnostní úrovně „vysoká“, naplní-li dopadová kritéria, může spadat do bezpečnostní úrovně „kritická“.
- **Informační nebo komunikační systém kritické informační infrastruktury** provozovaný jako celek prostřednictvím služeb cloud computingu spadá automaticky do bezpečnostní úrovně „kritická“.
- **Nejvyšší stanovená bezpečnostní úroveň informačního nebo komunikačního systému jako celku musí být stanovena alespoň pro jednu část informačního nebo komunikačního systému**, který je poptávaným cloud computingem. Jinak řečeno, systém zařazený např. v bezpečnostní úrovni „vysoká“ nejde dekomponovat na části, které budou všechny spadat pouze do bezpečnostních úrovní „nízká“ nebo „střední“.

[1] Viz § 4 odst. 7 vyhlášky o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.

3 Zařazení do bezpečnostní úrovně

3.1 Co je posuzováno a zařazováno do bezpečnostní úrovně?

Předmětem zařazování do odpovídající bezpečnostní úrovně je informační nebo komunikační systém jako celek, nebo jeho část, jenž mohou být provozovány pomocí cloud computingu. Tento systém nebo jeho část jsou definovány jako **poptávaný cloud computing**.

Je potřeba mít na paměti, že tato definice není stejná jako definice poptávaného cloud computingu podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů. Důvodem je, že v době vzniku návrhu vyhlášky užíval zákon o kybernetické bezpečnosti a zákon o informačních systémech veřejné správy pojem *„poptávaný cloud computing“* odlišně.

Poptávaným cloud computingem dle vyhlášky v žádném případě **není** konkrétní produkt, který by orgánu veřejné moci poskytovatel nabízel. U takového produktu z povahy věci nelze provést níže popsané posouzení.

Povinnost zařadit poptávaný cloud computing do odpovídající bezpečnostní úrovně dle zákona o kybernetické bezpečnosti se týká pouze systémů či jejich částí, které slouží k výkonu působnosti orgánu veřejné moci. Orgán veřejné moci nemusí do bezpečnostní úrovně zařazovat systém, prostřednictvím kterého není vykonávána působnost orgánu veřejné moci.

Co může být poptávaným cloud computingem:	Co nebude poptávaným cloud computingem:
Úřední deska	Textový editor (SaaS)
Informační systém pro správu místních poplatků	Databázový software (PaaS/SaaS)
Evidence uživatelů a žadatelů sociálních služeb	Konkrétní produkt úložiště (IaaS)
Modul pro uživatele (dekomponovaná část IS)	Webový nástroj konkrétního poskytovatele pro analýzu dat o návštěvnosti (PaaS/SaaS)

3.2 Základní principy a informace k zařazování

Obecně je úkolem správce vyhodnotit, jaké nejzávažnější dopady může mít případný kybernetický bezpečnostní incident v rámci posuzovaného informačního nebo komunikačního systému, a to v každé jednotlivé dopadové oblasti (jednotlivé sloupce tabulky v příloze č. 1 vyhlášky).

Správce přitom musí uvažovat nejhorší možné dopady z hlediska narušení **dostupnosti, důvěrnosti i integrity** v rámci posuzovaného systému a vzít v potaz jeho povahu jako celku. V případě, že do bezpečnostní úrovně zařazuje pouze část systému, musí taktéž zhodnotit vztah této části k systému 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:

1) **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.

2) **Identifikují se nejhorší možné „kritické“ scénáře.**

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

3) **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 analýze rizik dle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále jen „vyhláška o kybernetické bezpečnosti“).

4) **Neuvažují se existující bezpečnostní opatření.**

   Stěžejním principem celého hodnotícího procesu je hodnocení inherentních rizik, tedy že správce 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*.“.

3.2.2 Metoda hodnocení dopadů

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

Pro hodnocení dopadů v doménách dostupnosti, důvěrnosti a integrity je možné podpůrně postupovat dle metodického materiálu *Vodítka pro hodnocení dopadů*, který je dostupný na webových stránkách NÚKIB.

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.[2] 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 poptávaného cloud computingu do bezpečnostní úrovně

Požadavky na vyplnění hodnotícího 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 moci

Tato část formuláře obsahuje pouze identifikační údaje orgánu veřejné moci, který je správcem hodnoceného systému. Tuto část není třeba blíže rozebírat.

3.3.2 Část B: Identifikace informačního nebo komunikačního systému, jehož provozování je poptáváno pomocí cloud computingu

V následující části formuláře je třeba vyplnit základní údaje týkající se poptávaného cloud computingu, respektive hodnoceného systému. Důležité je zejména rozlišení, zda je řešení pomocí cloud computingu poptáváno pro systém jako celek, nebo jen pro jeho určitou vyčleněnou část (dílčí evidenci údajů, uživatelskou platformu, úložiště atp.). Pokud je poptávaným cloud computingem pouze část systému, pak je třeba tuto část systému určitým způsobem definovat a popsat její vztah k systému jako celku. Více informací k dekompozici částí systému lze nalézt ve Znalostní bázi k Architektuře eGovernmentu ČR.

B: Identifikace informačního nebo komunikačního systému, jehož provozování je poptáváno pomocí cloud computingu	
Označení systému:	*Evidence žadatelů a uživatelů soc. služeb*
Je řešení pomocí cloud computingu poptáváno pro informační nebo komunikační systém jako pro celek?	*Ne, pouze pro část*
V případě, že je řešení pomocí cloud computingu poptáváno jen pro část informačního nebo komunikačního systému, definujte ji z hlediska funkčních kategorií, architektury, provozního modelu a bezpečnosti:	
V této části může být popsána informační, aplikační či technologická architektura hodnocené části systému, respektive vazba této části na zbytek informačního systému, který není provozován prostřednictvím služeb cloud computingu.	

Při dekompozici systému na dílčí části je třeba pamatovat na ustanovení § 4 odst. 6 vyhlášky, ze kterého vyplývá, že **alespoň jedna z dekomponovaných částí systému, který je poptávaným cloud computingem, musí mít shodnou bezpečnostní úroveň, jako by měl systém jako celek**. Jinak řečeno, systém zařazený v bezpečnostní úrovni „vysoká“ nejde dokomponovat na části, které budou spadat pouze do bezpečnostních úrovní „nízká“ nebo „střední“.

[2] Viz § 4 odst. 7 vyhlášky o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.

3.3.3 Část C: Výsledná bezpečnostní úroveň

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

3.3.4 Část D: Zhodnocení bezpečnostní úrovně podle přílohy č. 1 vyhlášky

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

Konkrétní dopadová kritéria uvedená v příloze č. 1 vyhlášky jsou blíže vysvětlena v odůvodnění vyhlášky, které je dostupné na webových stránkách NÚKIB.

D: Zhodnocení bezpečnostní úrovně podle přílohy č. 1 vyhlášky		
Oblast dopadu	**Nejvyšší dosažená úroveň dopadu v příslušné oblasti**	**Odůvodnění**
A. Bezpečnost a zdraví lidí	z pohledu narušení dostupnosti	*Narušení dostupnosti, důvěrnosti či integrity Evidence žadatelů a uživatelů sociálních služeb (dále jen "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 poptávaný cloud computing, který naplňuje dvě 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.*
	NÍZKÁ	
	z pohledu narušení důvěrnosti	
	VYSOKÁ	
	z pohledu narušení integrity	
	VYSOKÁ	
C. Trestněprávní řízení	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. Řízení a provoz	z pohledu narušení dostupnosti	*Narušení dostupnosti, důvěrnosti či integrity Evidence může narušit řádné fungování části nebo celého Krajského úřadu Fiktivního kraje, přičemž může závažně omezit nebo zastavit provádění důležitých činností Krajského úřadu Fiktivního kraje.* *Konkrétně může dojít k omezení poskytování sociálních služeb a vyřizování žádostí o jejich poskytnutí. Zaměstnanci úřadu by při narušení dostupnosti vůbec neměli k evidenci přístup; při narušení integrity by taktéž došlo k zastavení předmětných činností, navíc by se toto narušení projevilo v dalších částech systému. V případě narušení důvěrnosti by k narušení činnosti úřadu a omezení vykonávání důležitých činností nedošlo.* *Nelze očekávat, že by došlo k narušení řízení, poškození rozvoje nebo poškození prosazování cílů a zájmů KÚ Fiktivního kraje, pročež nebude naplněna dopadová úroveň "vysoká".*
	STŘEDNÍ	
	z pohledu narušení důvěrnosti	
	NÍZKÁ	
	z pohledu narušení integrity	
	STŘEDNÍ	
G. Důvěryhodnost	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.*
	NÍZKÁ	

	z pohledu narušení důvěrnosti	*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 a žadatelů po narušení jejich integrity či důvěrnosti v důsledku kybernetického bezpečnostního incidentu.*
	STŘEDNÍ	
	z pohledu narušení integrity	
	STŘEDNÍ	
H. Finanční model	z pohledu narušení dostupnosti	*Běžné výdaje ročního rozpočtu Fiktivního kraje na rok 2021 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	
I. Zajišťování služeb	z pohledu narušení dostupnosti	*Průměrný počet uživatelů sociálních služeb a žadatelů o jejich poskytnutí činí za rok 2020 celkem 24849 osob. Průměrný meziroční nárůst počtu žadatelů a uživatelů se stabilně pohybuje do 5 %, v roce 2021 a dalších letech tak lze očekávat obdobný nárůst počtu uživatelů řešeného 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 hodnotící 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 systému v oblasti **B. Ochrana osobních údajů**, kde je dopadová úroveň „**vysoká**“, což znamená, že výsledná bezpečnostní úroveň hodnoceného systému bude taktéž „**vysoká**“. Tento závěr je třeba uvést do části C formuláře (viz výše).

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

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

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

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

Závěrem dotazníku je třeba vyplnit datum, ze kterého bude patrné, kdy ke zhodnocení systému došlo. Za příslušný orgán veřejné moci pak hodnotící formulář podepíše k tomu oprávněný zaměstnanec či jiná osoba, která byla příslušným orgánem veřejné moci pověřena k zařazení systému do odpovídající bezpečnostní úrovně. Jednou z příloh hodnotícího formuláře by měl být dokument prokazující oprávnění dané osoby k provedení hodnocení daného systému.

3.4 Specifika systému spadajících pod zákon o kybernetické bezpečnosti

Významné informační systémy dle § 4 odst. 4 vyhlášky automaticky spadají **minimálně do bezpečnostní úrovně „vysoká“**, pokud bude systém provozován prostřednictvím služeb cloud comutingu jako celek. Pokud by tímto způsobem fungovala pouze část významného informačního systému, je možné, že bude výsledná bezpečnostní úroveň nižší než „vysoká“. Na druhou stranu je možné, že významný informační systém jako celek splní dopadová kritéria pro kritickou úroveň dopadu a výslednou bezpečnostní úrovní tohoto systému tak bude také „kritická“ úroveň.

Obdobně **informační nebo komunikační systémy kritické informační infrastruktury**, které budou v celém svém rozsahu provozovány prostřednictvím služeb cloud computingu, spadají automaticky do bezpečnostní úrovně „kritická“.

3.5 Využití výstupů hodnocení

Hodnotící formulář je **písemným záznamem o procesu stanovení bezpečnostní úrovně** poptávaného cloud computingu dle § 4 odst. 7 vyhlášky, který dokládá splnění zákonné povinnosti vyplývající z § 4 odst. 5 zákona o kybernetické bezpečnosti, tedy zařazení poptávaného cloud computingu do bezpečnostní úrovně s ohledem na povahu dotčeného informačního nebo komunikačního systému před uzavřením smlouvy s poskytovatelem služeb cloud computingu.

Zjištěná bezpečnostní úroveň správci vymezuje, které konkrétní produkty zapsané v katalogu cloud computingu může v rámci svého informačního systému použít. Je-li posuzovaný informační systém 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. 181/2014 Sb., o kybernetické bezpečnosti
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy
- Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci
- Znalostní web odboru Hlavního architekta eGovernmentu ČR
- Národní architektonický plán a Národní architektonický rámec
- Materiály k Informační koncepci ČR – Řízení jednotlivých ICT řešení
- Materiály k Informační koncepci ČR – eGovernment cloud
- Materiály k Informační koncepci ČR – Dekompozice informačních systémů

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 **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**
30. listopadu 2021	1.0	OREG	Vytvoření dokumentu
5. ledna 2023	1.1	OREG	Změna kontaktních údajů