Metodika stanovení požadavků na bezpečnost IS

Příloha č. 4 Souhrnné analytické zprávy

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY
Ministerstvo financí České republiky
NÚKIB

Projekt Příprava vybudování eGovernment cloudu	
Fáze:	FÁZE I.(přípravná)

Úkol:	Předložit Vládě ke schválení souhrnnou analytickou zprávu v souladu se Strategickým rámcem Národního cloud computingu – eGovernment cloud ČR
Odpovědný subjekt:	Pracovní skupina RVIS pro přípravu vybudování eGovernment cloudu

Obsah

1 Úvodní informace k metodice

Účelem dokumentu je popsat metodiku a postup stanovení požadavků na bezpečnost informací zpracovávaných v rámci informačních systémů veřejné správy a dále z nich dekomponovaných ICT služeb, jejichž správcem jsou zákazníci eGC. Toto stanovení je založeno na hodnocení dopadů narušení bezpečnosti (dostupnost, důvěrnost, integrita).

Metodika je primárně určena pro organizační složky státu (OSS), může však být bez jakýchkoliv omezení použita i orgány územní samosprávy a ostatními zákazníky eGC.

Důvodem pro vznik této metodiky bylo nastavit jednotící kritéria (oblasti a úrovně dopadů, viz *Příloha A - Vodítka pro hodnocení dopadů*) a sjednotit postup stanovení požadovaných parametrů bezpečnosti při využívání služeb cloud computingu. A to z hlediska požadavků na dostupnost, důvěrnost a integritu. Metodika by měla správcům informačních systémů pomoci při rozhodování, které IS nebo jejich dekomponované ICT služby mohou migrovat do eGC, jakou úroveň bezpečnosti mají vyžadovat v rámci sdílených služeb, zda mohou využít služeb komerční nebo státní části eGovernment cloudu (eGC).

Metodika navazuje na „Metodiku k vodítkům pro hodnocení dopadů“ v1.2 z března 2018 (publikovaná na webu NÚKIB viz https://www.govcert.cz/cs/kyberneticky-zakon/podpurne-materialy/), vychází z obecných postupů a best practice (viz

Seznam použitých zdrojů) a je upravena na prostředí orgánů veřejné moci ČR.

2 Základní východiska

Hodnocení důležitosti informačních systémů veřejné správy se v souladu s touto metodikou hodnotí pomocí určení kritických dopadů narušení dostupnosti, důvěrnosti a integrity dat nebo ICT služby, na kterých je funkčnost hodnoceného IS závislá. Primárně se hodnotí celý IS, avšak v případě rozhodnutí o přechodu do eGC na některé nižší úrovni (PaaS, IaaS) nebo jen určité dekomponované ICT služby (plnící část funkčnosti IS) se provede hodnocení separátně pro tuto zajišťovanou ICT službu.

Pro určení dopadů narušení bezpečnosti je vytvořena hodnotící škála neboli vodítka hodnocení, která obsahují 10 oblastí (obecné scénáře) a 4 úrovně závažnosti dopadů (podrobněji viz *Příloha A - Vodítka pro hodnocení* dopadů). Použití jednotné škály (vodítek hodnocení) pro hodnocení různých informačních systémů, by mělo zajistit jednotný způsob posouzení závažnosti dopadů narušení bezpečnosti a zároveň umožnit srovnání výsledků v rámci veřejné správy.

Vymezení vůči zákonu č. 412/2005 Sb.

Metodika a vodítka hodnocení nejsou určená pro informační systémy nakládající s utajovanými informacemi dle zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti. Na sdílené infrastruktuře eGC (včetně státní části eGC) není reálné splnění požadavků prováděcích předpisů k zák. č. 412/2005 Sb. a tím i zpracování utajovaných informací dle tohoto zákona.

Vymezení vůči zákonu č. 181/2014 Sb.

V případě, že je v některém z parametrů bezpečnosti dosaženo úrovně dopadu “Vysoká”, popř. “Kritická” může správce zvážit zařazení informačního systému mezi významné informační systémy (VIS).

Průřezová kritéria pro určení prvku kritické infrastruktury dle §1 nařízení vlády č. 432/2010 Sb. budou ve většině případů odpovídat hodnocení dopadů IS nebo jeho dekomponované ICT služby v úrovni „kritická“ dle této metodiky.

3 Princip hodnocení dopadů

Stanovení požadavků na úroveň bezpečnostních opatření využívaných cloudových služeb je založeno primárně na identifikaci požadavků na bezpečnost a spolehlivost celého IS, případně na hodnocení dekomponované ICT služby. Požadavky na dekomponovanou ICT službu budou pravděpodobně ve většině případů shodné se zařazením celého IS, ale mohou z hodnocení vyjít i jako nižší, zejména v případě dekompozice funkčního rozsahu IS.

Určení bezpečnostních parametrů IS nebo dekomponované ICT služby vychází z identifikace kritických scénářů, které by mohly nastat v případě narušení dostupnosti zpracovávaných dat, jejich ztráty, narušení důvěrnosti a integrity dat. Kritické scénáře se pak mapují na scénáře uvedené ve vodítkách hodnocení (viz *Příloha A - Vodítka pro hodnocení dopadů*).

Hodnocení následků nedostupnosti

Hodnocení následků nedostupnosti vychází z předpokladu, že nedochází ke ztrátě dat, jen k jejich dočasné nedostupnosti způsobené výpadkem informačního systému. Následky vyplývající z nedostupnosti dat se mohou lišit v závislosti na délce nedostupnosti IS nebo dané ICT služby. Pro stanovení okamžiku, kdy se poprvé projeví dopady z nedostupnosti a jak se v čase vyvíjí, se hodnocení provádí v následujících časových intervalech.

- nedostupnost 15 min.
- nedostupnost 1 hod.
- nedostupnost 4 hod.
- nedostupnost 8 hod.
- nedostupnost 16 hod.
- nedostupnost 1 den
- nedostupnost 2 dny
- nedostupnost 1 týden
- nedostupnost 14 dní
- nedostupnost 1 měsíc a více

Určení dopadů v jednotlivých časových intervalech napomáhá identifikovat okamžik, kdy se již výpadek ICT služby stává pro správce IS neakceptovatelný. Je tak určující pro stanovení hodnoty RTO (recovery time objective), neboli času dokdy má být obnovena dostupnost služby po havárii.

Při hodnocení dopadů nedostupnosti je zároveň doporučeno zohlednit možnosti správce IS přejít na alternativní postupy zpracování dat – mimo systém, přičemž je ale třeba zohlednit sekundární dopady (např. zvýšené náklady), které zvolené alternativní zpracování může přinést.

Hodnocení narušení bezpečnosti dat a informací na základě interview s respondenty		Dostupnost									
Respondent	**Kategorie dat a informací (agenda)**	Nedostupnost 15 min.	Nedostupnost 1h	Nedostupnost 4h	Nedostupnost 8h	Nedostupnost 16 hod.	Nedostupnost 1den	Nedostupnost 2 dny	Nedostupnost 1 týden	Nedostupnost 14 dní	Nedostupnost měsíc a více
doplnit jméno respondenta	doplnit název AIS / kategorie dat a informací										
	Bezpečnost a zdraví osob										
	Ochrana osobních údajů										
	Zákonné a smluvní povinnosti										
	Trestně-právní řízení										
	Veřejný pořádek										
	Mezinárodní vztahy										
	Řízení a provoz organizace			1	1	1	1	1	2	2	2
	Ztráta důvěryhodnosti										
	Finanční ztráty									1	1
	Zajišťování nezbytných služeb										

Poznámka: U některých IS nebo ICT služeb se dopady nedostupnosti projeví v řádu minut až hodin, u jiných až v horizontu dní (obvykle pokud není daná agenda časově kritická, popř. lze její výkon zajistit mimo daný IS). Dopady nedostupnosti mohou u některých systémů růst lineárně, u některých bude dosaženo maxima např. po týdnu nedostupnosti a následně se již nezvětšuje (zůstává konstantní), protože se podařilo činnosti zajistit alternativním způsobem. Hlavní zásadou, kterou je třeba dodržovat, je že dopad v čase nemůže klesat.

Hodnocení následků ztráty dat

Tento dopad zkoumá následky, který by mohly vzniknout v případě ztráty dat. Pro určení optimálního požadavku na frekvenci zálohování dat se hodnocení provádí pro následující časové intervaly.

- Ztráta dat od zálohy (1 hod.)
- Ztráta dat od zálohy (4 hod.)
- Ztráta dat od zálohy (8 hod.)
- Ztráta dat od zálohy (16 hod.)
- Ztráta dat od zálohy (24 hod.)

Výsledek hodnocení totální ztráty dat ze systému může vyústit v požadavek na umístění záloh v geograficky oddělené lokalitě.

- Úplná ztráta dat

Hodnocení následků narušení důvěrnosti dat

Tento dopad je zkoumán z hlediska:

- prozrazení v rámci organizace – prozrazení zaměstnancům (lidem pracujícím pro organizaci, kteří však nemají oprávnění pro přístup k datům),
- prozrazení smluvním partnerům – prozrazení smluvním poskytovatelům služeb (zaměstnancům třetí strany, kteří mohou mít oprávněný přístup k systému nebo síti, ale nikoli k datům – například organizace provozující outsourcované informační služby),
- prozrazení vně organizace – únik informací na veřejnost.

Hodnocení narušení bezpečnosti dat a informací na základě interview s respondenty		Důvěrnost		
Respondent	**Kategorie dat a informací (agenda)**	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizaci
doplnit jméno respondenta	doplnit název AIS / kategorie dat a informací			
	Bezpečnost a zdraví osob			3
	Ochrana osobních údajů		2	3
	Zákonné a smluvní povinnosti			
	Trestně-právní řízení			
	Veřejný pořádek			
	Mezinárodní vztahy			
	Řízení a provoz organizace			
	Ztráta důvěryhodnosti	1		
	Finanční ztráty		2	3
	Zajišťování nezbytných služeb			

Hodnocení následků narušení integrity dat

Otázky zkoumané při vyšetřování tohoto dopadu se liší podle účelu hodnoceného informačního systému. Neodhalená změna nebo chyba v datech může způsobit zásadní dopady, organizace funguje na základě špatných dat. Dopad je zkoumán z hlediska:

- chyby malého rozsahu – neúmyslné modifikace dat, např. chyby při vkládaní dat uživatelem, duplikace vstupu,
- chyby velké rozsahu – narušení správnosti a úplnosti informací velkého rozsahu, např. chyby v kódu informačního systému, porušení integrity dat vlivem technické selhání,
- úmyslné modifikace – úmyslná změna provedená uživatelem nebo správcem systému.

Hodnocení narušení bezpečnosti dat a informací na základě interview s respondenty		Integrita		
Respondent	**Kategorie dat a informací (agenda)**	Modifikace dat malého rozsahu	Modifikace dat velkého rozsahu	Úmyslná modifikace
doplnit jméno respondenta	doplnit název AIS / kategorie dat a informací			
	Bezpečnost a zdraví osob	1	3	4
	Ochrana osobních údajů		1	2
	Zákonné a smluvní povinnosti			
	Trestně-právní řízení			
	Veřejný pořádek			
	Mezinárodní vztahy			
	Řízení a provoz organizace			
	Ztráta důvěryhodnosti		1	2
	Finanční ztráty		1	2
	Zajišťování nezbytných služeb			

4 Postup hodnocení dopadů

Osvědčenou metodou hodnocení dopadů je řízené interview s věcným správcem (garantem) daného informačního systému, případně ve spolupráci s bezpečnostním ředitelem. Interview je vedeno zkušeným analytikem, který je znalý metodiky a postupů kvalitativního a kvantitativního hodnocení dopadů. Obvyklá délka interview na jeden IS je 90 až 120 minut. V případě potřeby se interview po dohodě s věcným správcem doplní o další sezení. Pro hodnocení dekomponovaných ICT služeb bude třeba spolupráce s technickým správcem služby a s bezpečnostním ředitelem (případně zodpovědným pracovníkem za ICT bezpečnost). Dále používáme obecný termín „garant“ systému.

Provedení pilotních hodnocení na vybraném vzorku potenciálních zákazníků eGC ukázalo na potřebu minimálně první hodnocení dopadů provést formou řízeného interview pod metodickým vedením zkušeného analytika. U správců IS spadajících pod působnost zákona o kybernetické bezpečnosti toto bude v kompetenci bezpečnostní role manažera kybernetické bezpečnosti (manažera ISMS), popř. též architekta KB. Následné revize hodnocení pak již mohou garanti provádět samostatně. I zde je však doporučeno nezávislé posouzení výstupů analytikem. Zkušenost z provedených pilotních hodnocení ukázala, že ze strany garantů může docházet, byť k neúmyslnému, nadhodnocení, popř. podcenění dopadů z narušení bezpečnosti informačního systému. Pro většinu garantů bude tento způsob hodnocení dopadů nový, a proto je více než vhodné je při prvním hodnocení metodicky vést.

Záznam interview na hodnocení dopadů

Záznam hodnocení se provádí do připraveného Excel formuláře, viz obrázek níže. Excel formulář je k dispozici formou samostatného souboru.

Hodnocení narušení bezpečnosti dat a informací na základě interview s respondenty		Dostupnost										Ztráta						Důvěrnost			Integrita		
Respondent	**Kategorie dat a informací (agenda)**	Nedostupnost 15 min.	Nedostupnost 1h	Nedostupnost 4h	Nedostupnost 8h	Nedostupnost 16 hod.	Nedostupnost 1den	Nedostupnost 2 dny	Nedostupnost 1 týden	Nedostupnost 14 dní	Nedostupnost měsíc a více	Ztráta dat od zálohy (1hod.)	Ztráta dat od zálohy (4hod.)	Ztráta dat od zálohy (8hod.)	Ztráta dat od zálohy (16hod.)	Ztráta dat od zálohy (24hod.)	Úplná ztráta dat	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizaci	Modifikace dat malého rozsahu	Modifikace dat velkého rozsahu	Úmyslná modifikace
doplnit jméno respondenta	doplnit název AIS / kategorie dat a informací																						
	Bezpečnost a zdraví osob																						
	Ochrana osobních údajů																						
	Zákonné a smluvní povinnosti																						
	Trestně-právní řízení																						
	Veřejný pořádek																						
	Mezinárodní vztahy																						
	Řízení a provoz organizace																						
	Ztráta důvěryhodnosti																						
	Finanční ztráty																						
	Zajišťování nezbytných služeb																						
	Komentář k dopadům (uveďte odůvodnění k následkům narušení dostupnosti-odkdy a proč začíná mít nedostupnost negativní dopad, narušení důvěrnosti-např. porušení pravidel obecného nařízení GDPR, narušení integrity dat-např. chyba při zpracování dat agendy)																						

Průběh interview na hodnocení dopadů

V rámci interview jsou garanti dotazováni na nastínění realistického scénáře nejhoršího případu, který by mohl vyplývat z následujících dopadů:

- **nedostupnost** informačního systému (nedostupnost zpracovávaných informací),
- **ztráta** dat od poslední zálohy, úplná ztráta dat a informací,
- narušení **důvěrnosti** dat a informací (neoprávněné prozrazení a únik informací),
- narušení **integrity** dat a informací (vlivem neúmyslné modifikace (chyby), úmyslné modifikace dat a systémové chyby).

Interview zpravidla probíhají podle následujícího scénáře:

1) Získání základních informací o hodnoceném informačním systému: účel a rozsah zpracovávaných informací, relevantní legislativa a regulatorní požadavky, kritické termíny, úřední hodiny, lhůty apod.
2) Vysvětlení způsobu a postupu hodnocení dopadů. Zejména je potřeba zdůraznit dále uvedené zásady.
3) Kritické scénáře (scénáře nejhorší možného dopadu) popsané garantem se porovnají s obecnými vodítky pro hodnocení dopadů (viz *Příloha A - Vodítka pro hodnocení dopadů*). Pro určení závažnosti dopadů je použita stupnice o čtyřech úrovních dopadu (1-nízký, 2-střední, 3-vysoký, 4-kritický). *Poznámka: V případě, že se na danou situaci dá uplatnit více než jeden scénář současně (např. ohrožení bezpečnosti osob, ztráta důvěryhodnosti, finanční ztráta) se dopady nesčítají. Vždy se bere se v rámci vyhodnocení a stanovení požadavků na IS nebo dekomponované ICT služby v potaz nejvyšší dosažená úroveň dopadu pro každý z parametrů bezpečnosti, viz příklad uvedený na obrázku níže.*
4) Po zpracování výsledků interview je vhodné zaslat výstup z hodnocení garantovi k revizi a odsouhlasení provedeného hodnocení.

Hodnocení narušení bezpečnosti dat a informací na základě interview s respondenty		Dostupnost										Ztráta						Důvěrnost			Integrita		
Respondent	**Kategorie dat a informací (agenda)**	Nedostupnost 15 min.	Nedostupnost 1h	Nedostupnost 4h	Nedostupnost 8h	Nedostupnost 16 hod.	Nedostupnost 1den	Nedostupnost 2 dny	Nedostupnost 1 týden	Nedostupnost 14 dní	Nedostupnost měsíc a více	Ztráta dat od zálohy (1hod.)	Ztráta dat od zálohy (4hod.)	Ztráta dat od zálohy (8hod.)	Ztráta dat od zálohy (16hod.)	Ztráta dat od zálohy (24hod.)	Úplná ztráta dat	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizaci	Modifikace dat malého rozsahu	Modifikace dat velkého rozsahu	Úmyslná modifikace
doplnit jméno respondenta	doplnit název AIS / kategorie dat a informací																						
	Bezpečnost a zdraví osob											1	1	1	1	1	2			3	1	3	4
	Ochrana osobních údajů		1	2	2	2	2	3	3	3	3						1		2	3		1	2
	Zákonné a smluvní povinnosti																						
	Trestně-právní řízení																						
	Veřejný pořádek																						
	Mezinárodní vztahy																						
	Řízení a provoz organizace			1	1	1	1	1	2	2	2												
	Ztráta důvěryhodnosti			2	2	2	3	3	4	4	4						1	1				1	2
	Finanční ztráty									1	1			1	1	1	3		2	3		1	2
	Zajišťování nezbytných služeb																						

Zásady, které je třeba při hodnocení dodržovat

Podstatou hodnocení dopadů je určit důležitost informačního systému neboli stanovit skutečné požadavky na zajištění zpracovávaných dat z hlediska požadavků na jejich dostupnost, důvěrnost a integritu. Pro maximální objektivitu hodnocení je potřeba se držet následujících zásad:

- Při hodnocení dopadů se nezkoumají možné příčiny (hrozby) narušení bezpečnosti.
- Neurčuje se pravděpodobnost výskytu jednotlivých scénářů narušení dostupnosti, důvěrnosti, integrity. Pokud je dopad podle scénáře, byť jen minimálně pravděpodobný, bere se v potaz, a stanoví se možné dopady dle scénářů vodítek hodnocení.
- Vždy se posuzují nejhorší možné scénáře. Kritické scénáře popisují nejhorší možné, ale stále ještě pravděpodobné dopady, které by mohly nastat v důsledku realizace různých hrozeb (kybernetické hrozby, fyzické hrozby, technické závady atd.). *Např. výpadek systému v neděli dopoledne může být nezajímavý, v pondělí dopoledne již může způsobit negativní dopad na služby občanům.*
- Při hodnocení dopadů je důležité neuvažovat existující bezpečnostní opatření, aby se předešlo případným mylným předpokladům o jejich účinnosti a zejména pak zkreslení závažnosti dopadů.

5 Stanovení požadavků na bezpečnostní úroveň na základě výsledků hodnocení

Provedené hodnocení dopadů dává základ pro určení požadavků na bezpečnostní opatření. Například požadovanou úroveň redundance s ohledem na možné dopady nedostupnosti, požadavek na použití kryptografických prostředků na ochranu dat v případě vysokých dopadů v oblasti důvěrnosti a zajištění integrity dat při přenosu. Od takto stanovených požadavků se pak odvíjí volba cloudové služby (bezpečnostní úroveň v rámci eGC), která je schopna požadované bezpečnostní parametry garantovat.

Odvození požadavků na dostupnost služby

Při rozhodování o požadované úrovni bezpečnosti eGC bude pro většinu správců IS klíčovým kritériem požadavek na dostupnost. Na základě výsledků hodnocení v následku narušení dostupnosti lze odvodit základní požadavky na SLA služby, jak je uvedeno na obrázku níže.

Příklad: Pro IS nebo dekomponovanou ICT službu, která v následcích nedostupnosti dosáhne maximálně na střední úroveň dopadu a to až po 1 týdnu, bude dostačující SLA s garancí kumulovaného výpadku 8 hod. na měsíční bázi, tedy nejnižší úroveň eGC z hlediska dostupnosti.

Bezpečnostní úroveň	Základní požadavky na SLA cloudové služby			Dopady narušení dostupnosti									
	Dostupnost	Provozní doba pod SLA	Přípustná doba kumulovaných výpadků, s měsíčním vyhodnocováním	Nedostupnost 15 min.	Nedostupnost 1 h	Nedostupnost 4 h	Nedostupnost 8 h	Nedostupnost 16 hod.	Nedostupnost 1 den	Nedostupnost 2 dny	Nedostupnost 1 týden	Nedostupnost 14 dní	Nedostupnost měsíc a více
nízká (KeCG)	96,16%	Provozní doba pod SLA: minimálně určených 10 hodin v pracovní dny. Nezapočítávají se dny pracovního volna a dny pracovního klidu stanovené pro ČR. Např. r. 2018 má 250 pracovní dní , na bázi 10 hod. pod SLA denně, což dává max. měsíční výpadek 8,3 hod. při dostupnosti 96% (vztaženo na dobu pod SLA).	Max. 8 hod., avšak pouze v rámci definované pracovní doby	1							2	2	2
střední (KeCG)	99,45%	Provozní doba pod SLA: 24x7 (připravenost pro služby související s úplným el. podáním). Avšak určité služby SaaS, u nichž to lze předpokládat vzhledem k provozním aspektům, lze nabízet s omezením Provozní doby pod SLA na pracovní dny a vymezenou pracovní dobu. To znamená, že el. podání bude obvykle fungovat nepřetržitě, ale reakce poskytovatele na nahlášené incidenty je omezena.	Max. 4 hod. na bázi 24x7	1			2	2	2	3	3	3	3
vysoká (KeCG)	99,90%	Provozní doba pod SLA: 24x7 (připravenost pro služby úplného el. podání, a pro ISVS pod ZoKB). Určité služby SaaS, u nichž to lze předpokládat vzhledem k provozním aspektům, lze nabízet s omezením Provozní doby pod SLA na pracovní dny a vymezenou pracovní dobu.	Max. 43 min. na bázi 24x7	1		3	3	3	3	3	4	4	4
kritická (SeGC)	99,99%	Plně fault-tolerantní systém s geo-redundancí a replikací transakčních dat. Smluvní penále při výpadku dostupnosti služby delší než celkem 52 minut za rok (odpovídá 99,99%). Cloudové služby v této úrovni dopadu budou mít smluvně dané max. doby RPO / RTO.	Jednotlivý výpadek max. 15 min. Max. kumulovaný roční výpadek 52 min. (odpovídá 99,99%)	1-2			3-4						

Dosažení vyšší úrovně dopadů po delší době výpadku neznamená automaticky nutnost zařazení ICT služby do vyšší bezpečnostní úrovně eGC. Správce IS může vyhodnotit rezervu dostupnosti v SLA jako akceptovatelné riziko na základě předchozích statistik, že např. u SLA dostupnosti "vysoká" je velmi malá pravděpodobnost, že výpadek dosáhne reálně doby 1 týdne a tím úrovně dopadů "kritická". Každý správce IS musí vyhodnotit míru akceptovatelného rizika oproti zvýšeným nákladům, spojeným s pořízením služby kvalifikované pro vyšší úroveň dopadů.

Odvození požadavků na frekvenci vytváření a způsob uložení záloh dat

Pro časové intervaly, kde se dopady mění z hodnoty 1 na 2, popř. z hodnoty dopadu 2 na 3, je doporučeno vyjasnit výši nákladů, které mají zákazníci eGC s dodatečnou rekonstrukcí dat z jiných zdrojů (např. papírové formuláře) oproti nákladům spojeným s vyšší frekvencí vytváření záloh dat.

V případech, kdy jsou dopady z totální ztráty dat v elektronické podobě neakceptovatelné, je potřeby zvážit úroveň eGC, která nabízí geo-redundantní uložení dat.

Bezpečnostní úroveň	Ztráta dat					
	Ztráta dat od zálohy (1 hod.)	Ztráta dat od zálohy (4hod.)	Ztráta dat od zálohy (8hod.)	Ztráta dat od zálohy (16hod.)	Ztráta dat od zálohy (24hod.)	Úplná ztráta dat
nízká (KeCG)	Pro časové intervaly, kde se dopady mění z hodnoty 1 na 2, popř. z hodnoty dopadu 2 na 3 je doporučeno vyjasnit výši nákladů, které mají OVM s dodatečnou rekonstrukcí dat z jiných zdrojů (např. papírové formuláře) oproti nákladům spojeným s vyšší frekvecní vytváření záloh dat.					1
střední (KeCG)						2
vysoká (KeCG)						3
kritická (SeGC)						4

Stanovení požadavků na důvěrnost dat

Výběr požadované bezpečnostní úrovně eGC z hlediska požadavků na zajištění důvěrnosti dat bude zpravidla podřízen požadavkům na dostupnost. V případech, kdy je v parametru důvěrnost dosaženo vyšší úrovně dopadu než v oblasti dostupnosti, je bezpečnostní úroveň eGC volena na základě dosažené hodnoty dopadu v parametru důvěrnost. Pokud se tedy ještě neuplatní dopady za integritu dat, viz dále.

V případech, kdy je u hodnocených ICT služeb vyžadována ochrana právními předpisy, je nutné toto při výběru úrovně eGC zohlednit. Je-li tedy z nějakého důvodu ICT služba hodnocena dopadem ze ztráty důvěrnosti úrovní nižší než 3, je i přesto potřeba zvážit její zařazení do vyšší bezpečnostní úrovně eGC, minimálně do úrovně „vysoká“.

Poznámka: Bezpečnostní úrovně eGC jsou odstupňovány podle nabízených bezpečnostních funkcí zajišťujících důvěrnost uložených a přenášených dat. Pro úroveň dopadu „nízká“ nejsou kladené speciální požadavky na zajištění důvěrnosti a integrity dat. Naopak pro úroveň dopadu „vysoká“ a „kritická“ je nezbytné zajistit garanci šifrování uložených a přenášených dat, popř. také vyžadovat exkluzivní kontrolu nad šifrovacími klíči.

Bezpečnostní úroveň	Úrovně důvěrnosti		
	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizaci
nízká (KeCG)	1 Nízké požadavky na důvěrnost dat dle matice dopadů.		
střední (KeCG)	2 Střední požadavky na důvěrnost dat dle matice dopadů. V případech, kdy je vyžadována ochrana právními předpisy je nutné zvážit úroveň eGC "vysoká".		
vysoká (KeCG)	3 Vysoké požadavky na důvěrnost dat dle matice dopadů, popř. je ochrana vyžadována právními předpisy.		
kritická (SeGC)	4 Kritické požadavky na důvěrnost dat dle matice dopadů.		

Stanovení požadavků na integritu dat

Obdobně jako v oblasti důvěrnost platí i pro integritu dat, že výběr požadované bezpečnostní úrovně eGC bude zpravidla podřízen požadavkům na dostupnost ICT služby. Tam, kde je v parametru integrita dosaženo vyšší úrovně dopadu než v oblasti dostupnosti, popř. též důvěrnosti, je bezpečnostní úroveň eGC volena na základě dosažené hodnoty dopadu v oblasti integrity dat.

Bezpečnostní úroveň	Úrovně integrity		
	Neúmyslná modifikace (chyba)	Systémová chyba	Úmyslná modifikace
nízká (KeCG)	1 Nízké požadavky na integritu dat dle matice dopadů.		
střední (KeCG)	2 Střední požadavky na integritu dat dle matice dopadů.		
vysoká (KeCG)	3 Vysoké požadavky na integritu dat dle matice dopadů.		
kritická (SeGC)	4 Kritické požadavky na integritu dat dle matice dopadů.		

Služby v rámci jednotlivých úrovní eGC musí být nabízeny tak, aby mohly zajistit všechny parametry (dostupnost, důvěrnost, integrita) v dané úrovni dopadu. *Příklad: Pokud je zajišťovaná ICT služba v parametru dostupnost hodnocena úrovní 3-vysoká, v důvěrnosti 2-střední, v integritě 1-nízká, je zařazena do úrovně bezpečnosti eGC „vysoká“.* V případě, že by nabízené služby (v oblasti integrity a důvěrnosti) zákazník v některém aspektu plně nevyužil, může s poskytovatelem jednat o modifikaci služby a získání slevy.

Vysvětlení: Aby cloudové služby mohly přinést výhody z rozsahu, musí být provozovány jako multitenantní a vysoce škálovatelné. Nebylo by proto ekonomicky výhodné stavět oddělenou cloudovou infrastrukturu pro různé kombinace úrovní důvěrnosti, integrity a dostupnosti. Základní charakteristikou úrovně cloudové služby je zpravidla úroveň její dostupnosti a nabízeného SLA. Úrovně důvěrnosti a integrity lze někdy řešit jako dodatečné volby zabezpečení, které zákazník cloudové služby může, ale nemusí využít.

6 Závěr

Výsledky z provedeného hodnocení dopadů jsou pro správce IS vodítkem, jakou úroveň bezpečnostních opatření by měl interně zajistit, popř. vyžadovat v případě využití služeb eGC.

Zároveň by tyto výsledky měly správci pomoci při rozhodování, zda a za jakých podmínek může informační systém migrovat do eGC a jakou úroveň bezpečnosti eGC služeb požadovat.

Pro finalizaci hodnocení úrovní dopadů a zařazení příslušného IS nebo jeho dekomponované ICT služby do určité úrovně bezpečnosti eGC je vhodné provést kontrolu vedoucím pracovníkem zodpovědným za rozpočet organizace, zda finanční dopady a poměr cena/hodnota zabezpečení byly vyhodnoceny přiměřeně.

7 Příloha A - Vodítka pro hodnocení dopadů

Pro posouzení závažnosti dopadů způsobených narušením dostupnosti informačního systému veřejné správy, narušením důvěrnosti a integrity zpracovávaných dat jsou stanoveny následující oblasti dopadů.

A. Bezpečnost a zdraví osob
B. Ochrana osobních údajů
C. Zákonné a smluvní povinnosti
D. Trestně-právní řízení
E. Veřejný pořádek
F. Mezinárodní vztahy
G. Řízení a provoz organizace
H. Ztráta důvěryhodnosti
I. Finanční ztráty
J. Zajišťování nezbytných služeb

Závažnost dopadů je v každé z kategorií rozdělena do 4 úrovní dopadů (nízký, střední, vysoký a kritický). Matice dopadů je vytvořena tak, aby si úrovně (závažnosti) dopadů v jednotlivých kategoriích navzájem odpovídaly (byly přiměřeně korelovatelné). V případě, že je pro konkrétní případ hodnocení bezpečnosti dat poplatných více kategorií dopadů (např. je relevantní *Narušení bezpečnosti a zdraví osob* a *Ochrana osobních údajů*) použije se pro výsledné stanovení závažnosti dopadu nejvyšší dosažená hodnota v každém jednotlivém hodnoceném parametru bezpečnosti.

Pro další výklad a příklady použití jednotlivých oblastí dopadů se odkazujeme na Metodiku k vodítkům pro hodnocení dopadů v1.2 z března 2018 (publikovaná na webu NÚKIB viz https://www.govcert.cz/cs/kyberneticky-zakon/podpurne-materialy/),

Poznámka: Níže uvedená vodítka i formulář pro hodnocení dopadů jsou k dispozici formou samostatného Excel souboru.

Vodítka pro určení závažnosti dopadů narušení bezpečnosti informací (převzato z publikované metodiky NÚKIB v1.2 z března 2018)

Regulace odpovídající úrovni dopadu	Úroveň dopadu	Vodítka (oblasti) pro určení závažnosti dopadů narušení bezpečnosti informací (dostupnost, důvěrnost, integrita)								
		A. Bezpečnost a zdraví osob	B. Ochrana osobních údajů	C. Zákonné a smluvní povinnosti	D. Trestně-právní řízení	E. Veřejný pořádek	F. Mezinárodní vztahy	G. Řízení a provoz organizace	H. Ztráta důvěryhodnosti	I. Finanční ztráty	J. Zajišťování nezbytných služeb
Ostatní, ISVS, GDPR, ZKB - VIS, ISZS, ZKB - KII, ISZS	1 nízká	*žádné vodítko*	Může způsobit porušení etických, nikoli však právních předpisů vedoucí k negativním osobním dopadům na jednotlivce nebo skupinu osob.	Může zapříčinit porušení interních předpisů a postupů, nikoli však porušení zákonných a smluvních povinností.	*žádné vodítko*	*žádné vodítko*	*žádné vodítko*	Naruší řádné řízení nebo fungování části nebo celé organizace.	Může negativně ovlivnit vztahy s jinými částmi organizace, jinými organizacemi nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhé trvání.	Může přímo nebo nepřímo vést ke ztrátám menším než 0,05 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	*žádné vodítko*
	2 střední	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) jedné nebo několika osob.	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na jednotlivce (pokuta až 10 mil. EUR nebo 2 % celkového ročního obratu - viz čl. 83/4 GDPR).	Může zapříčinit správní nebo občanskoprávní řízení vedoucí k pokutě nebo k náhradě škody.	Může vytvořit podmínky pro páchání trestné činnosti nebo může ztížit její vyšetřování.	Může zapříčinit rozsahem, formou nebo místem omezené protesty (lokální nepokoje).	Může vytvářet negativní obraz ČR v jednom teritoriu, popř. v jednom státě.	Může omezit provádění důležitých činností organizace.	Může negativně ovlivnit vztahy s jinými organizacemi nebo veřejností, negativní publicita se ale bude týkat omezené zájmové skupiny nebo bude široká, avšak krátkodobá.	Může přímo nebo nepřímo vést ke ztrátám mezi 0,05 % a 2 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	Může způsobit závažné omezení či narušení nezbytných služeb pro malé množství osob.
	3 vysoká *	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) větší skupiny osob, nebo ohrožení na životě jednotlivců.	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na velkou skupinu osob (pokuta až 20 mil. EUR nebo 4 % celkového ročního obratu - viz čl. 83/5 GDPR).	Může zapříčinit porušení právních předpisů vedoucí k zahájení trestního stíhání.	Může vést k narušení vyšetřování trestné činnosti nebo soudní řízení (méně závažná kriminalita, krátkodobě, v jednotlivých případech).	Může zapříčinit rozsahem, formou nebo místem omezené protesty na úrovni významné části správního území obce s rozšířenou působností, jejichž řešení si může vyžádat aktivaci krizového řízení na úrovni kraje.	Může vytvářet negativní obraz ČR ve světě.	Může způsobit dočasné zastavení nebo podstatné narušení důležitých činností organizace nebo poškodit rozvoj nebo prosazování cílů a zájmů organizace.	Může závažně ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní negativní publicity.	Může přímo nebo nepřímo vést ke ztrátám vyšším než 2 % a nižším či rovným 10 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).Pozn. v případě PZS je hranice ztráty stanovena na 0,25 % HDP.	Může způsobit závažné omezení, narušení či nedostupnost nezbytných služeb pro více než 25 000 osob (v rámci kategorie provozovatelů základních služeb se může lišit dle právní úpravy pro jednotlivá odvětví viz vyhláška č. 437/2017 Sb.).
	4 kritická **	Může vést k přímému ohrožení či ztrátě života skupiny osob.	*žádné vodítko*	*žádné vodítko*	Může vést k závažnému, dlouhodobému narušení schopnosti vyšetřovat trestnou činnost, popřípadě zpochybnění soudních řízení a rozhodnutí (závažná kriminalita, celkové zpochybnění systému).	Může zapříčinit hromadné nepokoje, např. generální stávku, nebo jinak závažně narušit veřejný pořádek s celostátními dopady.	Může negativně ovlivnit nebo poškodit diplomatické vztahy a tím způsobit nevýhodu pro zájmy ČR.	Může závažně a dlouhodobě ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní či nadnárodní negativní publicity, s dlouhodobými účinky a požadavky přijetí politické odpovědnosti.	Závažně a dlouhodobě ovlivní vztahy s jinými organizacemi nebo veřejností s následkem celostátní či nadnárodní negativní publicity, s dlouhodobými účinky a požadavky přijetí politické odpovědnosti.	Může přímo nebo nepřímo vést ke ztrátám přesahujícím 10 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).Pozn. v případě KII je hranice ztráty stanovena na 0,5% HDP.	Může způsobit rozsáhlé omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.

8 Seznam použitých zdrojů

1) Strategický rámec Národního cloud computingu – eGovernment cloud ČR
2) Vodítka metodiky RAMSES (zejména profil vytvořený pro Národní bezpečnostní úřad), Risk Analysis Consultants, s.r.o.
3) ISO/IEC 27035:2016, Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response
4) Business Impact Level Tables, Extract from HMG IA Standard No. 1, Issue No: 3.5, October 2009, UK Cabinet Office
5) Zákon č. 365/2000 Sb. o informačních systémech veřejné správy a o změně některých dalších zákonů
6) Zákon č. č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti
7) Zákon č. 137/2001 Sb. o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením a o změně zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů
8) ISO 22317 – Societal Security – Business Continuity Management Systems – Business Impact Analysis
9) Metodika k vodítkům pro hodnocení dopadů v1.2 z března 2018, publikovaná na webu NÚKIB (https://www.govcert.cz/cs/kyberneticky-zakon/podpurne-materialy/),