MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Ministerstvo financí
České republiky

NÚKIB

Hodnocení úrovně bezpečnostních dopadů a zařazování do bezpečnostních úrovní eGC

Ing. Libor Široký, CISM, CRISC, AMBCI

RISK ANALYSIS CONSULTANTS

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Ministerstvo financí České republiky

NÚKIB

Hodnocení bezpečnostních dopadů IS

- **Hodnocení dopadů narušení bezpečnosti (C, I, A)**
  - ✓ určení bezpečnostních parametrů IS vychází z identifikace kritických scénářů
  - ✓ data nebo celé ICT služby, na kterých je funkčnost hodnoceného IS závislá
  - ✓ 10 obecných kritických scénářů dopadů (vodítka hodnocení)
  - ✓ závažnost dopadů (1-Nízká, 2-Střední, 3-Vysoká, 4-Kritická)
  - ✓ metodika je primárně určena pro organizační složky státu (OSS), může však být bez jakýchkoliv omezení použita i orgány územní samosprávy a ostatními zákazníky eGC
- **Mapování na vhodnou bezpečnostní úroveň služeb eGC**
  - ✓ stupnice (1-Nízká, 2-Střední, 3-Vysoká, 4-Kritická)
  - ✓ kategorizace úrovně bezpečnostních opatření služeb eGC
  - ✓ základní východisko při rozhodování o umístění do KeGC / SeGC

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Ministerstvo financí České republiky

NÚKIB

Hodnocení bezpečnostních dopadů IS (princip)

- **Nezkoumají se příčiny (hrozby) narušení bezpečnosti**
- **Neurčuje se pravděpodobnost výskytu jednotlivých scénářů**
- **Posuzují nejhorší možné „kritické“ scénáře**
- **Neuvažují se existující bezpečnostní opatření**
- **Hodnocení je založeno na identifikaci požadavků na bezpečnost celého IS, případně dekomponované ICT služby**
  - ✓ Požadavky na dekomponovanou ICT službu budou pravděpodobně ve většině případů shodné se zařazením celého IS

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Ministerstvo financí České republiky

NÚKIB

Hodnocení bezpečnostních dopadů IS (postup)

- **interview s věcným správcem (garantem) daného informačního systému, popř. také technickým správcem služby u dekomponovaných ICT služeb**
- **délka interview na jeden IS je 90 až 120 minut**
- **nastínění realistického scénáře nejhoršího případu:**
  - ✓ 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 (neúmyslné modifikace (chyby), úmyslné modifikace dat a systémové chyby)
- **vyhodnocení scénáře dle vodítek hodnocení**
- **záznam hodnocení se provádí do připraveného formuláře**

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Ministerstvo financí České republiky

NÚKIB

Kontext bezpečnostních opatření vůči legislativě

- **Vymezení vůči zákonu č. 412/2005 Sb.**
  - ✓ Metodika eGC hodnocení bezpečnostních dopadů není určená pro IS nakládající s utajovanými informacemi dle zák. č. 412/2005 Sb.
- **Vymezení vůči zákonu č. 181/2014 Sb.**
  - ✓ Jestliže je v některé z oblastí dopadů dosaženo úrovně "Vysoká", popř. "Kritická" může správce zvážit zařazení IS mezi **VIS/KII/PZS** za dalších podmínek (nv. 432/2010 Sb., v. 437/2017 Sb., v. 317/2014 Sb.)
- **Vymezení vůči Obecnému nařízení GDPR**
  - ✓ Požadavky na zpracování osobních údajů v cloudových službách musí dle nařízení GDPR vycházet z hodnocení rizik daného scénáře zpracování pro práva a svobody fyzických osob.
  - ✓ V případě zjištění vysokého rizika jsou správci povinni provést tzv. „posouzení vlivu zpracování dat na ochranu osobních údajů" (DPIA, viz čl. 35), a zajistit adekvátní bezpečnostní opatření a mechanismy ochrany, a to **bez ohledu na možné využití eGC**.

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Ministerstvo financí České republiky

NÚKIB

Vodítka hodnocení bezpečnostních 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**

Úroveň dopadu		A. Bezpečnost a zdraví osob	B. Ochrana osobních údajů	C. Zákonné a smluvní povinnosti
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.
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.
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.
4	kritická **	Může vést k přímému ohrožení či ztrátě života skupiny osob.	*žádné vodítko*	*žádné vodítko*

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Ministerstvo financí České republiky

NÚKIB

Hodnocení bezpečnostních dopadů IS

- **Vodítka dopadů je vytvořena tak, aby si úrovně (závažnosti) dopadů v jednotlivých scénářích navzájem odpovídaly – byly přiměřeně korelovatelné**

- **V případě, že je poplatných více scénářů dopadů použije se nejvyšší dosažená hodnota**

Úroveň dopadu		Vodítka (kategorie) pro určení závažnosti dopadů narušení bezpečnosti informací (dostupnost, důvěrnost, integrita) - NUKIB v1.0 / 23.02.2018									
		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
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*	Může narušit 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*

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Ministerstvo financí České republiky

NÚKIB

Hodnocení bezpečnostních dopadů IS (dostupnost)

- **Hodnocení nedostupnosti vychází z předpokladu, že nedochází ke ztrátě dat, jen k jejich dočasné nedostupnosti.**
- **Určení dopadů v jednotlivých časových intervalech napomáhá identifikovat okamžik, kdy se již výpadek IS stává neakceptovatelný.**

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										
	Bezpečnost a zdraví osob										
	Ochrana osobních údajů		1	2	2	2	2	3	3	3	3
	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
	Finanční ztráty									1	1
	Zajišťování nezbytných služeb										

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Ministerstvo financí České republiky

NÚKIB

Hodnocení bezpečnostních dopadů IS (ztráta)

- **Pro určení požadavku na frekvenci ZÁLOHOVÁNÍ dat se hodnocení dopadů provádí v časových intervalech.**
- **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.**

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

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Ministerstvo financí České republiky

NÚKIB

Hodnocení bezpečnostních dopadů IS (důvěrnost)

- **DŮVĚRNOST je zkoumána z hlediska prozrazení v rámci organizace, prozrazení smluvním partnerům, prozrazení vně organizace**

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			
	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			

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Ministerstvo financí České republiky

NÚKIB

Hodnocení bezpečnostních dopadů IS (integrita)

- **INTEGRITA zkoumá následky neúmyslné a úmyslné modifikace informací**

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			
	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			

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Ministerstvo financí České republiky

NÚKIB

Výsledné hodnocení dopadů narušení bezpečnosti IS

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																						

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Ministerstvo financí České republiky

NÚKIB

Stanovení požadavků na bezpečnostní úroveň eGC

Bezpečnostní úroveň	Základní požadavky na SLA cloudové služby			Dopady narušení dostupnosti										Ztráta dat						Úrovně důvěrnosti			Úrovně integrity		
	Dostupnost	Provozní doba pod SLA	Přípustná doba kumulovaných výpadků, s měsíčním vyhodnocováním	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	Neúmyslná modifikace (chyba)	Systémová chyba	Úmyslná modifikace
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	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 frekvencí vytváření záloh dat.						1	1 Nízké požadavky na důvěrnost dat dle matice dopadů.			1 Nízké požadavky na integritu dat dle matice dopadů.		
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								2	2 Střední požadavky na důvěrnost dat dle matice dopadů. V případech, kdy je vyžadována ochrana právními předpisy je nutné zvážit úroveň eGC "vysoká".			2 Střední požadavky na integritu dat dle matice dopadů.		
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								3	3 Vysoké požadavky na důvěrnost dat dle matice dopadů, popř. je ochrana vyžadována právními předpisy.			3 Vysoké požadavky na integritu dat dle matice dopadů.		
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															4	4 Kritické požadavky na důvěrnost dat dle matice dopadů.			4 Kritické požadavky na integritu dat dle matice dopadů.		

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Ministerstvo financí České republiky

NÚKIB

Příklady hodnocení bezpečnostních dopadů IS

- **Spisová služba**
- **Agendový informační systém**