Metodický pokyn

Ministerstva financií Slovenskej republiky

č. MF/012943/2012-165

pre hodnotenie bezpečnostných štandardov

1. Úvod

Metodický pokyn poskytuje návod pre hodnotenie bezpečnostných štandardov podľa výnosu Ministerstva financií Slovenskej republiky č. 312/2010 Z. z. (ďalej len „výnos MF SR“), ktorý bol vydaný na základe zákona č. 275/2006 o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o IS VS).

Cieľom metodického pokynu je umožniť správne pochopenie jednotlivých požiadaviek bezpečnostných štandardov a zároveň dosiahnuť čo možno najpresnejšie odpovede pri ich hodnotení.

2. Metodika výpočtu hodnotenia

Na vypracovanie percentuálneho hodnotenia dodržiavania konkrétnych štandardov, ako aj výsledného hodnotenia celej oblasti bezpečnostných štandardov bol zavedený systém váhovania – jednotlivé trestné body sa vypočítavajú v pomere k váhe, pričom stupnica váh má tri úrovne:

1. Základná – bodová hodnota 1
2. Zvýšená – bodová hodnota 2
3. Vysoká – bodová hodnota 3

V osobitných prípadov existuje aj váha o hodnote 0,5, a to najmä pre rozdelené časti jednej požiadavky.

Počas hodnotenia sa pri zistení nedostatkov udeľujú tzv. trestné body, ktoré sa rozdeľujú na tri úrovne:

- dodržanie – neudeľuje sa žiadny trestný bod
- čiastočné dodržanie (mierne porušenie) – udeľuje sa polovica váhy danej požiadavky (v prípade váhy 1 je to teda 0,5)
- nedodržanie (vážne porušenie) – udeľuje sa plná váha.

Hodnotenie sa vykonáva vo forme otázok zástupcovi prípadne zástupcom kontrolovanej organizácie, pričom pravdivosť tvrdení si je možné overiť na základe rôznych skutočností, ktoré sú uvedené v poznámke pre hodnotiteľa.

Pri kontrole sa hodnotí splnenie požiadavky danej konkrétnym štandardom, nie však kvalita alebo forma prevedenia – tieto sa obvykle uvádzajú iba v poznámke k hodnoteniu,

pričom je možné v prípade nevhodnosti prevedenia odporúčať jej zlepšenie. V prípadoch, kde nie je možné jednoznačne určiť logickú odpoveď áno / nie sa zvažuje, či bola dodržaná podstata danej požiadavky.

Výsledné hodnotenie kontroly vyjadruje percentuálne dodržiavanie bezpečnostných štandardov, ktoré je kategorizované takto:

Výsledné hodnotenie	**Slovná kategória**
100%	Dodržiava
99 – 90%	Významne dodržiava
89 – 70%	Čiastočne dodržiava
69 – 50%	Porušuje
49 – 25%	Vážne porušuje
24 – 10%	Veľmi vážne porušuje
9% – 0%	Nedodržiava (zásadne porušuje)

3. Podklady potrebné k overeniu dodržiavania štandardov

Pri hodnotení je potrebné mať k dispozícii všetku relevantnú dokumentáciu, a to aj takú, ktorá sa informačnej bezpečnosti týka iba okrajovo, čo napomôže overiť systémové (formálne) zavedenie štandardov a zároveň záujem a znalosti organizácie ich implementovať.

Z hlavných dokumentov sú to najmä:

- bezpečnostná politika,
- bezpečnostný projekt,
- vnútorné smernice pre narábanie s informačnými systémami a informačno-komunikačnými prostriedkami,
- havarijné plány / plány na obnovu,
- dokumentácia jednotlivých informačných systémov,
- atď.

Zo sekundárnych dokumentov sú to najmä:

- vnútorné predpisy ohľadom nástupu a odchodu zamestnanca,
- vnútorné predpisy ohľadom disciplinárneho konania, resp. povinnosti, viažuce sa k dodržiavaniu vnútorných predpisov a procesov organizácie,
- prikladná zmluva, týkajúca sa informačných systémov,
- atď.

Štruktúra dokumentov je v jednotlivých organizáciách odlišná. Citovaný výnos Ministerstva financií Slovenskej republiky požiadavku na štruktúru nedefinuje. Jedinou výnimkou je požiadavka na existenciu jedného „zastrešujúceho“ dokumentu, ktorý je hierarchicky nadradený ostatným dokumentom. V niektorých prípadoch však môže existovať

iba jeden konzistentný dokument, ktorý pokrýva všetko, v iných prípadoch to môže byť množstvo rôznych vzájomne prepojených dokumentov a príloh. Návod pre hodnotenie je preto potrebné chápať tak, že obsahom bezpečnostnej politiky sa rozumie aj obsah ľubovolného relevantného dokumentu. Dokumenty nemusia mať striktne písomnú podobu – najmä pre niektoré flexibilne a často sa meniace požiadavky informačnej bezpečnosti je vhodnejšia elektronická podoba (napr. správa používateľských účtov).

Overovanie sa okrem dokumentácie môže týkať aj praktickej existencie technologických riešení a zavedenia bezpečnostných opatrení, organizačných postupov a ich znalosti. Z pohľadu praxe je dôležitejšie mať bezpečnostné opatrenia implementované ako formalizované (napr. zaužívané postupy či vedomosti systémových administrátorov), z pohľadu zachovania kontinuity činnosti organizácie to už nie je také jednoznačné (najmä pre prípady výmeny alebo nedostupnosti zodpovedných zamestnancov, krízové situácie a bezpečnostné incidenty, potrebu zmeny informačných systémov a podobne).

4. Metodika hodnotenia

4.1 Legenda k tabuľke hodnotiteľa

Otázky označené tmavším podkladom a zároveň bez uvedenia čísla a váhy nie sú bodované a majú iba doplňujúci charakter.

- Stĺpec „Číslo [Váha]“ označuje príslušné ustanovenie, ktorým je daná požiadavka definovaná a číslo v zátvorke uvádza priradenú váhu.
- Stĺpec „Požiadavka“ definuje odporúčanú kontrolnú otázku.
- Stĺpec „Predpoklad odpovede“ popisuje predpokladaný spôsob odpovedania na kontrolnú otázku.

  Predpoklad odpovede „áno / nie“ znamená zaznamenanie logickej odpovede na danú otázku, táto automaticky obsahuje aj možnosť odpovede „čiastočne“.

  V prípade popisných odpovedí sa nedodržanie odporúča popisovať vo forme „nie je zavedené / implementované“ atď.
- Stĺpec „Poznámka pre hodnotiteľa“ navrhuje spôsoby overovania kontrolnej otázky a zápisu odpovede.
- Stĺpec „Záznam“ je určený na zápis výsledkov kontroly.

Prílohou metodického pokynu je aj jednoduchý formulár, ktorý Ministerstvo financií Slovenskej republiky používa pri vykonávaní kontroly. Tento okrem vyššie uvedených častí obsahuje aj stĺpec pre záznam kontroly, zápis trestných bodov a percentuálneho hodnotenia dodržiavania jednotlivých štandardov.

4.2 Tabuľka hodnotiteľa

Číslo [Váha]	Požiadavka	Predpoklad odpovede	Poznámka pre hodnotiteľa	Záznam
[3]	**§ 28 Riadenie informačnej bezpečnosti**			
§28a) [2]	1. Existuje bezpečnostná politika (BP)?	[áno / nie]	*Overuje sa fyzická existencia dokumentu. Samotný dokument môže mať iný názov, ale musí to byť hierarchicky najvyšší dokument, týkajúci sa celej informačnej bezpečnosti organizácie.*	
	Ak je to relevantné, je táto politika rezortná alebo iba organizácie?	[rezortná / organizácie]	*Zapisuje sa slovná odpoveď.*	
	Je schválená v rámci procesov organizácie ?	[áno / nie]	*Overuje sa podpis relevantnej riadiacej osoby prípadne vykonanie schvaľovacieho procesu.*	
	Ak áno, kedy bola schválená?	[dátum]	*Overuje sa dátum schválenia.*	
	Akým spôsobom (na akej úrovni)?	[popis formy schválenia s identifikáciou príslušného dokumentu]	*Zapisuje sa pozícia (funkcia) schvaľovateľa.*	
§28a) 1 [1]	2. Sú určené bezpečnostné ciele?	[áno (+ počet cieľov a slovný popis) / nie]	*Overuje sa obsah BP.*	
§28a) 2 [1]	3. Sú určené spôsoby ich vyhodnocovania alebo dosahovania? Ak áno, ako?	[áno / nie]	*Overuje sa obsah BP.*	
	Na základe čoho boli určené?	[slovný popis prípadne zdroj]	*Overuje sa ústna odpoveď. V prípade vychádzania z existujúcej normy sa táto uvádza.*	

§28a) 3 [1]	4. Obsahuje podporu vedenia?	[áno / nie]	*Overuje sa existencia vyhlásenia o podpore vedenia resp. podpis vedúceho pracovníka (v rámci schvaľovacieho procesu podľa bodu 1) a zavedenie v rámci vnútorných predpisov.*	
§28a) 4 [1]	5. Sú stanovené pozície pre manažment informačnej bezpečnosti?	[áno (+ popis kategórií / názvov funkcií) / nie]	*Overuje sa obsah BP. V súvislosti s bodom 18 sa overuje popis kompetencií a povinností, vyplývajúcich z týchto pozícií. V súvislosti s bodom 17 je možné overiť aj obsadenosť daných pozícií a náplň práce.*	
§27a) 6 [1]	6. Ako je vyhodnotený a zabezpečený súlad bezpečnostnej politiky s ostatnými právnymi dokumentmi?	[vecný popis]	*Overuje sa obsah BP (existencia vzťahu k iným právnym dokumentom), prípadne vykonávaná činnosť.*	
§28a) 7 [1]	7. Ako sa požiadavky, vyplývajúce z právnych dokumentov premietli do správy IS VS?	[vecný popis]	*Overuje sa prijatý postup. Je možné overiť aj príslušnú dokumentáciu.*	
§28a) 8 [1]	8. Sú stanovené úrovne ochrany IS VS?	[áno / nie]	*Overuje sa obsah BP (existencia rozlíšenia bežných, t.j. nepodstatných častí IS VS a citlivých, resp. kritických častí).*	
	Ako sú definované?	[zoznam úrovní]	*Overuje sa obsah BP. V zázname sa uvádza iba názov úrovní, overuje sa aj rozlíšenie ich ochrany.*	
§28a) 9 [1]	9. Sú definované aktíva, ktoré súvisia s IS VS?	[áno / nie]	*Overuje sa obsah BP.*	
	Sú definované kritické aktíva? Ktoré to sú ?	[áno / nie]	*Overuje sa obsah BP. Postačuje skupinové určenie.*	

§28a) 10 [1]	10. Je stanovený rozsah a periodicita auditu informačnej bezpečnosti?	[áno / nie]	*Overuje sa obsah BP.*	
	Ako často sa audit vykonáva?	[časová periodicita]	*Overuje sa obsah BP a overuje sa aj skutočné vykonanie auditov (záznam z auditu).*	
	Vykonáva sa interne alebo externe?	[interne / externe]	*Overuje sa obsah BP a prípadne záznam z auditu.*	
§28a) 11 [1]	11. Sú vypracované smernice pre zálohovanie?	[áno / nie]	*Overuje sa fyzická existencia dokumentov. Môžu byť aj súčasťou BP.*	
	Ak áno, existuje rozdelenie údajov pre rôzne typy záloh?	[áno / nie]	*Overuje sa obsah BP. Typy záloh nemusia striktne zohľadňovať názvy podľa výnosu MF SR, musia ich však zohľadňovať principiálne.*	
	Aká periodicita bola zvolená pre prevádzkovú zálohu a aká pre archivačnú?	[časová periodicita]	*Overuje sa obsah BP.*	
	Ako je postihované nedodržiavanie týchto smerníc?	[vecný popis]	*Overuje sa obsah BP, prípadne iných súvisiacich vnútorných predpisov.*	
§28a) 12 [0,5]	12. Ako často sa vykonáva monitorovanie bezpečnosti softvéru?	[časová periodicita]	*Overuje sa obsah BP. Môže sa overiť aj vykonanie samotného monitorovania, resp. jeho výsledky. Monitorovanie nie je auditom, ale najmä priebežnou činnosťou zodpovedných administrátorov.*	
[0,5]	13. Ako často sa vykonáva aktualizácia softvéru?	[časová periodicita]	*Overuje sa obsah BP a zavedená politika pre aktualizáciu.*	
§28a) 13 [1]	14. Existuje zoznam dokumentov na zaistenie informačnej bezpečnosti?	[áno / nie]	*Overuje sa obsah BP.*	
	Ktoré dokumenty to sú?	[vymenovať zoznam]	*Overuje sa obsah BP.*	

	Sú tieto dokumenty vypracované?	[áno / nie]	*Overuje sa fyzická existencia dokumentov.*	
	Ak áno, kedy boli vypracované?	[dátum]	*Overuje sa dátum vypracovania.*	
	Boli tieto dokumenty aktualizované?	[áno / nie]	*Overuje sa procesný postup.*	
	Ak áno, kedy a s akou periodicitou?	[dátum poslednej aktualizácie, prípadne časová periodicita]	*Overuje sa buď obsah BP, obsah daných dokumentov alebo skutočný proces.*	
§28a) 14 [1]	15. Je stanovený postup revízie bezpečnostnej politiky?	[áno / nie]	*Overuje sa obsah BP.*	
	Ako často sa revízia vykonáva?	[časová periodicita]	*Overuje sa obsah BP. Je možné overiť aj proces skutočného vykonania revízie v súlade s obsahom BP.*	
	Aké dôvody boli stanovené na mimoriadnu revíziu?	[stručný slovný popis]	*Overuje sa obsah BP.*	
§28 b) [3]	16. Sú stanovené postupy v prípade nedodržiavania bezpečnostnej politiky?	[áno / nie]	*Overuje sa obsah BP, prípadne ďalších vnútorných predpisov.*	
	Akým spôsobom?	[slovný popis]	*Overuje sa obsah BP, prípadne ďalších vnútorných predpisov.*	
§28 c) [3]	17. Je stanovená osoba(y) zodpovedná(é) za informačnú bezpečnosť?	[áno (popis pozície) / nie]	*Overuje sa pozícia určenej osoby a skutočná fyzická osoba; môže sa overiť aj povedomie danej fyzickej osoby, ktoré mu z tejto pozície vyplýva, t.j. čo táto povinnosť znamená (podľa nasledovného bodu). Pri viacerých osobách sa toto určuje pre každú osobitne. V prípade určenia fyzickej osoby nezávisle od pozície sa zisťujú dôvody takéhoto*	

			konania.	
§28 d) [2]	18. Aké úlohy má osoba, zodpovedná za informačnú bezpečnosť?	[stručný slovný popis]	*Overuje sa obsah BP, prípadne opis práce.*	
§28 e) [1]	19. Ako je zabezpečená koordinácia aktivít organizačných zložiek pri riešení informačnej bezpečnosti?	[názov predpisu, podľa ktorého konanie nastáva, prípadne slovný popis]	*Overuje sa existencia smerníc/predpisov a príslušných kompetencií; je možné aj náhodne overiť znalosť postupov zodpovedných riadiacich pracovníkov v niektorom z týchto útvarov. Predpisom môže byť aj BP.*	
§28 f) [1]	20. Sú určené konkrétne zodpovedné osoby / útvary za jednotlivé aktíva?	[áno (vymenovanie) / nie]	*Overuje sa existencia zoznamu aktív a útvarov / pozícií (napr. v BP) a pridelených osôb.*	
§28 g) [1]	21. Ako sú určené bezpečnostné pozície v IS VS?	[slovný popis]	*Vyhodnocuje sa všeobecné určenie pozícií (rolí), pričom je možné vyhodnocovať aj pre každý IS VS osobitne. Vyhodnocujú sa aj bezpečnostné požiadavky na dané pozície a popis právomocí.*	
[2]	**§ 29 Personálna bezpečnosť**			
§29 a) [1]	22. Je zabezpečené poučenie o BP a povinnostiach z nej vyplývajúcich?	[áno / nie]	*Overujú sa zavedené postupy. Je možné overiť aj tlačivo o poučení, ak existuje.*	

	Ako sa vykonáva poučenie o BP a povinnostiach z nej vyplývajúcich?	[stručný slovný popis]	*Overuje sa existencia procesov prípadne dokumentov.*	
	Ako sa zabezpečuje poučenie osôb, ktoré vykonávajú činnosti na základe zmluvných vzťahov?	[stručný slovný popis]	*Overuje sa existencia procesov prípadne dokumentov (najmä zmlúv).*	
§29 b) [1]	23. Ako je zabezpečené poučenie o právach a povinnostiach pred vstupom do IS VS?	[stručný slovný popis]	*Overuje sa existencia procesov prípadne dokumentov. Overuje sa rozdielnosť postupov pre rôzne IS VS.*	
§29 c) [1]	24. Sú povinnosti vyplývajúce z BP uvedené v pracovných zmluvách príslušných zamestnancov?	[áno / nie]	*Overuje sa implementácia najmenej v jednej relevantnej pracovnej zmluve. Overuje sa aj spôsob zahrnutia relevantných povinností pri volených funkciách.*	
§29 d) [2]	25. Existuje vypracovaný postup pre disciplinárne konanie v prípade porušenia BP alebo relevantných predpisov?	[áno / nie]	*Overuje sa existencia takéhoto postupu (najmä samostatné konanie alebo vzťah k všeobecným vnútorným predpisom).*	
§29 e) [1]	26. Ako je zabezpečená povinnosť oznamovať bezpečnostné incidenty?	[stručný vecný popis]	*Overuje sa zavedenie v BP, vnútorných predpisoch alebo pri poučení. Je možné overiť aj znalosť tejto povinnosti na náhodne vybraných zamestnancoch.*	
§29 f) [2]	27. Sú vypracované postupy pri ukončovaní práce či pracovného pomeru, ktoré zabezpečujú ochranu IKT v správe organizácie?	[áno / nie]	*Overuje sa zavedenie vo vnútorných predpisoch prípadne v rámcovej pracovnej zmluve (či osobitných prac. zmluvách). Overuje sa zahrnutie útvaru informatiky do procesu ukončenia prác.*	

	Ktoré oblasti pokrývajú?	[zoznam oblastí]	*Uvádzajú sa oblasti podľa § 28 f) 1 až 5 (mlčanlivosť, odovzdanie pridelených zariadení, odstránenie údajov zo zariadení, zrušenie prístupových práv, odovzdanie agendy).*	
[2]	**§ 30 Manažment rizík pre oblasť informačnej bezpečnosti**			
§30 a) [1]	28. Existuje implementovaný systém riadenia rizík?	[áno / nie]	*Overuje sa zavedenie v relevantnom dokumente a zavedenie praktických postupov. Analýza rizík je podkladom pre riadenie, nie však samotným riadením.*	
	Ako je implementovaný?	[slovný popis]	*Zvažuje sa, či existuje klasifikácia rizík, zavedenie zostatkových rizík, zavedenie postupov.*	
[1]	29. Existuje implementovaný systém monitorovania rizík?	[áno / nie]	*Overuje sa zavedenie v relevantnom dokumente a zavedenie praktických postupov. Odporúča sa overiť na konkrétnom riziku, ktoré bolo identifikované v BP alebo inom dokumente.*	
	Ako je implementovaný?	[slovný popis]	*Zvažuje sa, či sú implementované mechanizmy na monitorovanie rizík a ako sa spracovávajú.*	
§30 b) [1]	30. Používa sa systém riadenia rizík a monitorovania ?	[áno / nie]	*Overuje sa náhodnou otázkou na niektorý náhodný proces ohľadom spôsobu použitia. Je možné overovať aj vzhľadom na hypotetickú zmenu v procese riadenia informačnej bezpečnosti.*	
	Ak nie, kde sa nepoužíva a prečo?	[slovný popis]	*Zapisuje sa dôvod.*	

§30 c) [1]	31. Zohľadňujú riziká aj aktíva a IS VS mimo priestorov povinnej osoby?	[áno / nie]	*Overuje sa zahrnutie takýchto rizík do relevantného dokumentu, a to najmä pre organizácie, ktoré majú distribuované pracoviská.*	
	Aké postupy sú zvolené na ich redukciu?	[slovný popis]	*Overuje sa náhodný jeden postup. Vyhodnocuje sa iba existencia.*	
§30 d) [2]	32. Existuje analýza závislosti na IS VS?	[áno / nie]	*Overuje sa relevantný dokument, ktorý popisuje uvedenú závislosť, a to najmä z procesného hľadiska. Uvedený dokument by mal byť základom pre KRIS, resp. zavádzanie elektronických služieb.*	
	33. Existuje analýza kritických procesov?	[áno / nie]	*Overuje sa relevantný dokument, v ktorom je zoznam kritických procesov.*	
§30 e) [2]	34. Existuje analýza (zoznam) kritických informačných systémov?	[áno / nie]	*Súvisí s predchádzajúcou otázkou. Overuje sa existujúci zoznam.*	
	Sú riziká pre ne špecificky oddelené?	[áno / nie / niektoré]	*Overuje sa relevantný dokument. Riziká pre kritické IS by mali mať odlišné dopady.*	
§30 f) [1]	35. Existujú vypracované plány na obnovu?	[áno / nie]	*Overuje sa ich existencia (v súlade s nasledovnou podotázkou).*	
	Ktoré plány sú vypracované?	[zoznam]	*Overuje sa existencia uvedených plánov. Výber môže byť napr. nasledovný: havarijný plán, plán na následnú obnovu (obmedzený mód), obnova kontinuity činnosti (úplný mód). Plány môžu byť aj zjednotené v jednom dokumente.*	
[2]	**§ 31 Kontrolný mechanizmus riadenia informačnej bezpečnosti**			
§31 a) [2]	36. Vykonáva sa vnútorná kontrola alebo audit informačnej bezpečnosti?	[áno / nie]	*Overuje sa vykonanie posledného auditu – dátum vykonania sa zapisuje. Je možné overiť aj dodržiavanie periodicity*	

			definovanej v bezpečnostnej politike.	
	Je vykonávaný interne alebo externe?	[interne / externe]		
§31 b) [1]	37. Sú auditné správy archivované? Sú chránené? Sú vyhodnocované?	[áno / nie]	*Overuje sa existencia archívnych správ. Overuje sa aj spôsob ich ochrany a vyhodnocovania.*	
[2]	**§ 32 Ochrana proti škodlivému kódu**			
§32a) 1 [1]	38. Je zavedená ochrana e-mailov? (škodlivý kód atď.)	[áno / nie]	*Pre skutočné overenie je potrebná fyzická kontrola.*	
§32a) 2 [1]	39. Je zavedená detekcia škodlivého kódu na zariadeniach IS SV?	[áno / nie]	*Pre skutočné overenie je potrebná fyzická kontrola.*	
§32a) 3 [1]	40. Sú kontrolované zasielané a prijímané súbory?	[áno / nie]	*Pre skutočné overenie je potrebná fyzická kontrola.*	
§32a) 4 [1]	41. Je zavedená ochrana webových sídiel a kontrola existencie škodlivého kódu?	[áno / nie]	*Pre skutočné overenie je potrebná fyzická kontrola. Overenie sa vykonáva najmä v používanom redakčnom systéme (CMS) a súvisiacich logoch.*	
§32 b) [1]	42. Je zavedená ochrana pred nevyžiadanou elektronickou poštou?	[áno / nie]	*Pre skutočné overenie je potrebná fyzická kontrola.*	
	Aký princíp používa?	[slovný popis]	*Rozlišuje sa spamový kôš používateľa, automatické blokovanie, hybridné riešenia atď.*	
§32 c) [1]	43. Je zavedená kontrola legality softvéru, používaného používateľmi?	[áno / nie]	*Overuje sa existujúca procedúra prípadne vnútorný predpis, ktorý sa týka správy inštalácií softvéru. V prípade automatizovaných foriem kontroly je možné overiť aj funkčnosť konkrétnej aplikácie.*	
§32 d) [1]	44. Existujú pravidlá pre sťahovanie súborov	[áno / nie]	*Overuje sa existencia pravidiel. Je možné aj náhodne overiť znalosť používateľov*	

	z externých sietí?		*o existencii takýchto pravidiel. Pravidlá sa majú týkať najmä ilegálnych alebo zakázaných formátov súborov.*	
§32 e) [1]	45. Existuje podpora kryptografických prostriedkov autenticity a integrity? Používa sa v IS inštitúcie elektronický podpis?	[áno / nie]	*Overuje sa existencia vnútorného predpisu prípadne priamo implementácie v systéme (pokiaľ je automatizovaná). Overuje sa aj poskytnutie možnosti kryptovania elektronickej komunikácie.*	
	Je povinná (aspoň pre určité prípady nakladania s údajmi)? Ak áno, pre ktoré?	[vecný popis]	*Overuje sa existencia procedúr.*	
	Je dodržiavaná?	[vecný popis]	*Overuje sa znalosť dodržiavania, resp. existencia overovania implementácie tohto bezpečnostného pravidla.*	
§32 f) [1]	46. Existuje podpora šifrovania elektronických dokumentov?	[áno / nie]	*Overuje sa existencia vnútorného predpisu prípadne priamo implementácie v systéme (pokiaľ je automatizovaná). Overuje sa aj v súlade s bodom 88.*	
	Je povinná (aspoň pre určité prípady nakladania s údajmi)? Ak áno, pre ktoré?	[zoznam, vecný popis]	*Overuje sa existencia vo vnútorných predpisoch alebo automatické zavedenie systémom.*	
	Je dodržiavaná?	[vecný popis]	*Overuje sa znalosť dodržiavania resp. existencia overovania tohto bezpečnostného pravidla.*	
[1]	**§ 33 Sieťová bezpečnosť**			
§33 a) [2]	47. Existuje implementácia firewallov?	[áno / nie]	*Pre skutočné overenie je potrebná fyzická kontrola.*	
	Sú nasadené iba ochrany vonkajšieho perimetra alebo aj personálne firewally?	[áno / nie, vecný popis]	*Overuje sa rozlíšenie prístupu ochrany voči vonkajšiemu a vnútornému prostrediu. Pre skutočné overenie je potrebná fyzická kontrola.*	

	Ak existujú aj personálne firewally, v akom rozsahu sú nasadené?	[vecný popis]	*Overuje sa pravidlo, podľa ktorého sa takáto implementácia uskutočňuje.*	
§33 b) [1]	48. Je vedená evidencia o všetkých miestach prepojení sietí v správe povinnej osoby (tzv. uzly)?	[áno / nie]	*Overuje sa existencia príslušného dokumentu, resp. schémy. Je možné ju viesť iba v elektronickej forme.*	
	Je aktualizovaná?	[áno / nie]	*Overuje sa proces aktualizácie.*	
§33 c) [1]	49. Je pre každé miesto podľa písm. b) vypracovaný interný akt riadenia prístupu?	[áno / nie]	*Overuje sa existencia interného(ých) aktu(ov). Môžu existovať aj univerzálne akty riadenia pre viaceré miesta.*	
[2]	**§ 34 Fyzická bezpečnosť a bezpečnosť prostredia**			
§34 a) [2]	50. Sú IS VS alebo aspoň ich kritické komponenty umiestnené v zabezpečenom priestore?	[áno / nie]	*Overuje sa fyzická existencia daného priestoru. Je možné aj overenie ochrany pred vplyvmi prostredia, pred haváriami technickej infraštruktúry, pred vstupom nepovolaných osôb.* *Zároveň sa overuje fyzické umiestnenie serverov v tomto priestore.*	
§34 b) [2]	51. Je tento priestor zabezpečený fyzickými prostriedkami?	[áno / nie]	*Overuje sa v súlade s predchádzajúcim bodom. Overuje sa nedostupnosť nepovolaným osobám.*	
§34 c) [1]	52. Je tento priestor umiestnený dostatočne ďaleko od ohrozenia fyzickými prostriedkami (kanalizácia, vodovod, horľaviny atď.)?	[áno / nie]	*Overuje sa fyzické rozmiestnenie kanalizácie, vodovodov, skladov horľavín, dostatočná klimatizácia, možnosť vytopenia atď. Overenie konštrukčných plánov nie je dostačujúce, je však možné dodatočné porovnanie.*	
§34 d) [1]	53. Existujú pravidlá pre prácu v zabezpečenom priestore?	[áno / nie]	*Overuje sa existencia pravidiel, a to najmä vo vnútorných predpisoch.*	

§34 e) [2]	54. Je zabezpečená ochrana pred výpadkom elektriny?	[áno / nie]	*Overuje sa fyzická existencia sekundárnych zdrojov prípadne záložných serverov. Overuje sa aj rozsah zabezpečenia pracovných staníc.*	
§34 f) [1]	55. Existujú záložné kapacity IS VS? Ak áno, aké sú (čo presne je zálohované)?	[áno (vecný popis) / nie]	*Overuje sa fyzická existencia záložných kapacít (sekundárnych alebo virtualizovaných serverov, kabeláž, atď.)*	
	Sú umiestnené v sekundárnom zabezpečenom priestore, dostatočne vzdialenom od pôvodného?	[áno / nie]	*Overuje sa fyzická existencia sekundárneho priestoru a umiestnenie záložných kapacít. Môže sa vyskytovať aj v tej istej budove.*	
§34 g) [1]	56. Je prevádzka, používanie a manažment IS VS v súlade s legislatívou, vnútornými predpismi a zmluvami? Ako je to docielené?	[áno / nie]	*Overuje sa spôsob zabezpečenia súladu. Samotná poskytnutá odpoveď naznačuje znalosti dôležitých procesov a požiadaviek a ich zavedenie do praxe.*	
§34h) 1 [1]	57. Existujú pravidlá pre údržbu, uchovávanie a evidenciu technických komponentov IS VS?	[áno / nie]	*Overuje sa existencia príslušného dokumentu. Je možné overiť aj zavedenie a spôsob kontroly.*	
§34h) 2 [0,5]	58. Existujú pravidlá pre používanie zariadení IS VS na iné účely?	[áno / nie]	*Overuje sa existencia príslušného dokumentu. Je možné overiť aj na konkrétnom príklade (napr. použitie serveru pre webové sídlo aj inými aplikáciami funkcie, prípadne používanie virtualizácie serverov).*	
§34h) 3 [0,5]	59. Existujú pravidlá pre prenos a používanie zariadení IS VS mimo určených priestorov (v rámci organizácie)?	[áno / nie]	*Overuje sa existencia príslušného dokumentu (väčšinou vo vzťahu k správe majetku). Je možné overiť aj na konkrétnom príklade (napr. notebooky, USB kľúče).*	

§34h) 4 [1]	60. Existujú pravidlá pre vymazávanie, vyraďovanie a likvidáciu zariadení IS VS a záloh?	[áno / nie]	*Overuje sa existencia príslušného dokumentu. Je možné aj overenie postupu na konkrétnom príklade (napr. odchod zamestnanca, repasácia atď.). Je možné aj fyzické overenie pokusu o obnovu informácií na vyradenom zariadení alebo zálohe.*	
§34h) 5 [1]	61. Existujú pravidlá pre prenos zariadení IS VS mimo priestorov organizácie?	[áno / nie]	*Overuje sa existencia príslušného dokumentu. Úzko súvisí s bodom 59 – overenie je možné spojiť. Je možné aj fyzické overenie pokusom o prenos zariadenia mimo priestorov organizácie.*	
§34h) 6 [0,5]	62. Existujú pravidlá pre narábanie so všetkými informáciami v elektronickej podobe (aj pri prevode z a do písomnej podoby), dokumentáciou systému a pamäťovými médiami?	[áno / nie]	*Na náhodnom type informácie je možné overiť spôsob ochrany pred neoprávneným zverejnením, odstránením, poškodením alebo modifikáciou (napr. výstup z alebo vstup do IS VS). Špeciálny dôraz je kladený na USB prípadne fotoaparáty mobilných zariadení.*	
§34 i) [1]	63. Je stanovená maximálna prípustná doba výpadku IS VS?	[áno / nie]	*Overuje sa obsah príslušného dokumentu. Overuje sa najmä pre kritické informačné systémy.*	
	Ak áno, aká doba to je a v ktorom dokumente je stanovená?	[slovná odpoveď]		
[0,5]	64. Aké opatrenia sú stanovené na riešenie obnovy prevádzky v prípade výpadku?	[zoznam]	*Overuje sa obsah príslušného dokumentu. Je možné overenie znalosti správcov jednotlivých IS VS o uvedenom postupe. Je možné aj fyzické overenie výpadku a obnovy niektorej časti IS VS.*	
[1]	**§ 35 Aktualizácia softvéru**			

§35 a) [1]	65. Je zabezpečená aktualizácia verzií inštalovaného ochranného softvéru? Ak áno, pre ktoré typy softvéru je zabezpečená?	[áno / nie]	*Overuje sa existencia postupov aktualizácie. Je možné overiť aj zmluvné a fyzické nastavenie aktualizácií.*	
§35 b) [1]	66. Je táto aktualizácia v súlade s BP?	[áno / nie]	*Overuje sa zahrnutie aktualizácie do BP, resp. preukázanie, že nie je v kolízii.*	
[1]	**§ 36 Monitorovanie a manažment bezpečnostných incidentov**			
§36a) 1 [2]	67. Je vypracovaný interný akt pre ohlasovanie bezpečnostných incidentov?	[áno / nie]	*Overuje sa existencia relevantného dokumentu. Súvisí s bodom 26.*	
§36a) 2 [1]	68. Je vypracovaný interný akt pre riešenie a vyhodnocovanie typov bezpečnostných incidentov?	[áno / nie]	*Overuje sa existencia relevantného dokumentu.*	
§36a) 3 [1]	69. Je vypracovaný interný akt pre spôsob evidencie bezpečnostných incidentov a použitých riešení?	[áno / nie]	*Overuje sa existencia relevantného dokumentu. Súvisí s predchádzajúcim bodom a s bodom 71 a môže byť súčasťou spoločného dokumentu. Je možné overiť aj existenciu zoznamu evidovaných bezpečnostných incidentov.*	
§36 b) [1]	70. Je zabezpečené informovanie používateľov IS VS o postupoch pri hlásení bezpečnostných incidentov?	[áno / nie]	*Overuje sa existencia relevantného dokumentu prípadne vykonaných školení. Je možné overiť aj existenciu relevantného tlačiva / formulára.*	
	Ak áno, akým spôsobom? Akým spôsobom je zabezpečovaná kontrola dodržiavania týchto postupov?	[vecný popis]	*Overuje sa vhodnosť resp. praktická uskutočniteľnosť informovania a kontroly. Je možné overiť znalosť náhodne vybraných používateľov o týchto postupoch.*	

§36 c) [2]	71. Existuje evidencia každého výpadku a spôsobu jeho riešenia?	[áno / nie]	*Overuje sa existencia evidencie (v prípade neexistencie je možné overiť identifikované incidenty).*	
§36 d) [1]	72. Je zavedený systém na detekciu prienikov (najmenej IDS)?	[áno / nie]	*Táto otázka sa overuje iba pre povinné osoby podľa §3 ods. 1 písm. a). Overuje sa fyzická existencia systému.*	
§36 e) [2]	73. Existuje kontaktné miesto na ohlasovanie bezpečnostných incidentov a slabých miest?	[áno / nie]	*Overuje sa fyzická existencia kontaktného miesta a dostupnosť (zverejnenie) kontaktov.*	
	Je možné ohlásiť aj bezpečnostný incident, identifikovaný externe?	[áno / nie]	*Overuje sa zverejnenie do externého prostredia.*	
[1]	**§ 37 Periodické hodnotenie zraniteľnosti**			
§37 a) [1]	74. Vykonáva sa periodické hodnotenie slabých miest IS VS (najmenej raz za rok)?	[áno / nie]	*Overuje sa záznam z posledného hodnotenia. Overuje sa príslušné znenie v BP, prípadne spôsob vykonávania.*	
[1]	**§ 38 Zálohovanie**			
§38 a) [2]	75. Existujú archivačné a prevádzkové zálohy podľa BP (prevádzková aspoň raz za týždeň, archivačná aspoň raz za 2 mesiace)?	[áno / nie]	*Overuje sa fyzická existencia záloh.*	
§38 b) [1]	76. Má archivačná záloha dve kópie?	[áno / nie]	*Overuje sa fyzická existencia druhej kópie.*	
§38 c) [1]	77. Vykonáva sa test funkcionality dátového nosiča jednotlivých záloh?	[áno / nie]	*Overuje sa existencia danej procedúry. Náhodne sa overuje možnosť čítania údajov zo starších záloh.*	
§38 d) [1]	78. Vykonáva sa test obnovy systému zo zálohy (najmenej raz za rok)?	[áno / nie]	*Overuje sa záznam z testu a zároveň periodicita testovania.*	
[1]	**§ 39 Fyzické ukladanie záloh**			

§39 a) [1]	79. Sú zálohy a licencovaný softvér ukladané v uzamykateľnom priestore?	[áno / nie]	*Overuje sa fyzická existencia priestoru a uloženie záloh.*	
§39 b) [1]	80. Ukladá sa druhá kópia archivačnej zálohy v inom objekte?	[áno / nie]	*Overuje sa popis daného miesta. Iný objekt môže byť aj súčasťou tej istej budovy. Je možné overiť fyzickú existenciu daného miesta a uloženia záloh.*	
[2]	**§ 40 Riadenie prístupu**			
§40 a) [3]	81. Je zavedená identifikácia a autentizácia pri vstupe do všetkých IS VS?	[áno / nie]	*Overujú sa náhodné systémy a spôsob prihlasovania.*	
	Aká úroveň sa bežne používa? Existujú pre niektoré systémy aj vyššie úrovne?	[slovná odpoveď]	*Overuje sa zavedenie úrovní typu meno+heslo, grid karta, jednorázové SMS heslo, biometrika a podobne.*	
§40 b) [2]	82. Je vypracovaný interný akt riadenia prístupu k údajom a funkciám ISVS?	[áno / nie]	*Overuje sa existencia interného aktu, resp. všeobecného zavedenia diferencovaných prístupových práv.*	
	Aký princíp používa?	[vecný popis]	*Overuje sa zavedenie princípu obmedzenia prístupu iba k potrebným údajom napr. na základe rolí – tento sa overuje v danom dokumente na základe vecných skutočností.*	
§40 c) [1]	83. Existuje postup a určená zodpovednosť pre prideľovanie prístupových práv?	[áno / nie]	*Overuje sa existencia osoby zodpovednej za pridelenie prístupu a existencia zavedeného postupu (napr. na základe žiadosti, podpísanej nadriadeným).*	
§40 d) [1]	84. Sú určené bezpečnostné požiadavky pre používateľov pri používaní IS VS?	[áno / nie]	*Overuje sa existencia príslušného predpisu (prípadne implementovaných upozornení v systéme). Je možné overiť súlad s BP. Je možné náhodne overiť*	

			znalosť používateľov. Odlišné IS VS môžu mať odlišné požiadavky.	
§40 e) [1]	85. Sú zmeny prístupu automaticky zaznamenávané a archivované?	[áno – dátum záznamu / nie]	*Overuje sa existencia záznamu, resp. archívu. Môže súvisieť so zabezpečením bodu 88.*	
§40 f) [1]	86. Existujú bezpečnostné zásady pre mobilné pripojenie?	[áno – názov dokumentu / nie]	*Overuje sa existencia príslušného dokumentu alebo zásad. Aj úplný zákaz je zásada. Overujú sa ako zásady pre mobilné zariadenia, tak pre mobilný prístup mimo priestorov organizácie.*	
§40 g) [1]	87. Je zavedená kontrola, že používatelia nepoužívajú IS VS na nelegálne účely?	[áno / nie]	*Overuje sa spôsob kontroly. Je možné overiť relevantný záznam (napr. aj v elektronickej podobe).*	
§40 h) [2]	88. Je zabezpečené, aby administrátori nemali prístup k údajom, ktoré nepotrebujú na vykonávanie svojich úloh?	[áno / nie]	*Overuje sa existencia šifrovania údajov, oddelenie správy používateľov alebo systému od prístupu k údajom, zavedenie sankcií a podobne. Overuje sa najmä vo vzťahu k tretím stranám. Je možné overiť aj fyzické zavedenie.*	
§40 i) [2]	89. Existuje automatické zaznamenávanie prístupu všetkých používateľov a správcov IS VS do systému?	[áno / nie]	*Overuje sa fyzická existencia záznamov. Je možné overiť vo viacerých IS VS.*	
	Sú zaznamenávané aj činnosti? Ak áno, aké typy a v akom rozsahu?	[slovný popis]	*Zapisujú sa zaznamenávané kategórie činností.*	
[1]	90. Ako je zamedzené vymazanie záznamov (bez schválenia zodpovednou	[vecný popis]	*Overuje sa existencia relevantného postupu a implementovaného riešenia, napr. zasielanie sekundárnej kópie*	

	osobou)?		*bezpečnostnému manažérovi.*	
§40 j) [1]	91. Je zavedená formalizovaná dokumentácia prístupových práv všetkých používateľov IS VS?	[áno / nie]	*Overuje sa existencia dokumentácie (môže byť aj v elektronickej podobe). Je možné overiť pre viac IS VS.*	
[2]	**§ 41 Aktualizácia informačno-komunikačných technológií**			
§41 a) [3]	92. Je zavedený schvaľovací proces pre zmeny existujúcich a zavádzanie nových ISVS a IKT, ktorý zároveň zahŕňa bezpečnostné požiadavky?	[áno / nie]	*Overuje sa relevantný dokument. Je možné overiť aj použitie postupu pri niektorej z posledných zmien či návrhov IS VS.*	
§41 b) [1]	93. Je zabezpečené menovanie zástupcu organizácie pre činnosti podľa predchádzajúceho bodu?	[áno / nie]	*Overuje sa existencia pre niektorú z prebiehajúcich činností. Je možné overiť menovanie v už ukončených činnostiach.*	
§41 c) [1]	94. Existuje zabezpečenie menovania zástupcu dodávateľa?	[áno / nie]	*Overuje sa zavedenie v dodávateľskej zmluve prípadne iným spôsobom.*	
	Ako je zabezpečené?			
§41 d) [2]	95. Bolo pri každej zmene existujúceho alebo zavádzaní nového IS VS vykonané testovanie v dostatočnom rozsahu (min. 1 týždeň)?	[áno / nie]	*Overuje sa existencia dokumentácie o testovaní. Zapisuje sa aj priemerná doba testovania. Je možné overiť v príslušnom procesnom dokumente, týkajúcom sa zmeny / zavádzania náhodne zvoleného IS VS.*	
§41e) 1 [1]	96. Existuje ku každému IS VS používateľská dokumentácia (návod na používanie)?	[áno / nie]	*Overuje sa existencia príslušnej dokumentácie pre jeden alebo viac IS VS.*	

§41e) 2 [1]	97. Existuje ku každému IS VS administrátorská dokumentácia (návod na správu a prevádzku)?	[áno / nie]	*Overuje sa existencia príslušnej dokumentácie pre jeden alebo viac IS VS.*	
§41e) 3 [1]	98. Existuje ku každému IS VS prevádzková dokumentácia (architektúra, konfigurácie a väzby)?	[áno / nie]	*Overuje sa existencia príslušnej dokumentácie pre jeden alebo viac IS VS.*	
[2]	**§ 42 Účasť tretej strany**			
§42 a) [1]	99. Je vykonávaná analýza rizík v súvislosti s dodávateľskými prácami?	[áno / nie]	*Overuje sa existencia analýzy pre náhodne zvolené IS VS a činnosti. Overuje sa v súlade s bodmi 28 až 34.*	
§42 b) [3]	100. Sú v zmluvách s dodávateľmi zahrnuté bezpečnostné požiadavky?	[áno / nie]	*Overujú sa náhodné zmluvy. Bezpečnostné požiadavky zahŕňajú napr. bezpečnostné štandardy podľa výnosu MF SR, zabezpečenie ochrany diela pred nevyžiadanými funkciami, neobmedzujúce nastavenie autorských práv, ochrana osobných údajov, dodržiavanie BP organizácie, mlčanlivosť atď.*	
§42 c) [3]	101. Je zamedzené alebo zmluvne zabezpečené, aby dodávatelia nemali prístup k údajom, ktoré sú aktíva podľa BP?	[áno / nie]	*Overuje sa implementácia alebo zmluva pre náhodne vybrané IS VS. Je možné overiť pre viac IS VS. Prístup môže byť udelený na základe zmluvy pri riešení určených činností či incidentov.*	
§42 d) [2]	102. Sú zmluvne vyžadované bezpečnostné požiadavky kontrolované? Ak áno, ako?	[áno – vecný popis / nie]	*Overuje sa vykonanie a spôsob kontrol.*	
§42 e) [3]	103. Je zmluvne zabezpečené, aby nedodržanie bezpečnostných požiadaviek zo strany	[áno / nie]	*Overujú sa náhodné zmluvy.*	

	dodávateľa umožnilo neukončiť alebo neprebrať jeho dielo alebo prácu?			

5. Záver

Upozornenie:

Informácie, ktoré sa týkajú informačnej bezpečnosti a rôznych nastavení a informačných systémov sú citlivé, a preto je potrebné vhodne zvažovať, komu môžu byť poskytnuté.

Ministerstvo financií SR v tomto prípade nemôže v zmysle zákona č. 275/2006 Z. z. delegovať právomoc na vykonanie kontroly inej organizácii ako vlastnému zamestnancovi ministerstva.

Komunikácia:

V prípade nejasnosti výkladu ľubovoľnej časti tohto metodického pokynu je k dispozícii e-mailová adresa standard@mfsr.sk, kde je možné prípadné otázky konzultovať.

Miloš Molnár, MBA
generálny riaditeľ
sekcie informatizácie spoločnosti