HODNOCENÍ RIZIKA

Hodnocené podpůrné aktivum (předmět dodávky)	Primární aktivum[1]	Hodnocení důležitosti primárního aktiva	Hodnocení důležitosti podpůrného aktiva[2]			Primární cíl hrozby	Hrozba[3]	Zkratka	Hodnocení závažnosti hrozby[2]	Hodnocení závažnosti dopadů (tj. dopad porušení důvěrnosti, dostupnosti nebo integrity aktiva)[2] [1]										Riziko, včetně korekce hodnocením primárního aktiva[2]
			Důvěrnost	Dostupnost	Integrita					Bezpečnost a zdraví osob	Ochrana osobních údajů	Zákonné a smluvní povinnosti	Trestně-právní řízení	Veřejný pořádek	Mezinárodní vztahy	Řízení organizace	Ztráta důvěryhodnosti	Finanční ztráty	Zajišťování nezbytných služeb	
služby v oblasti vývoje software, nezahrnující podporu a údržbu software	*Primární aktivum 1*	*Hodnocení 1*				Technická aktiva (hardwarové a softwarové vybavení, média a dokumenty)[4]	porucha zařízení nebo chybné fungování aplikačního programového vybavení	H1													0
	Primární aktivum 2	*Hodnocení 2*					nedbalostní nebo úmyslné poškození, chyba použití	H2													0
	Primární aktivum 3	*Hodnocení 3*					ztráta, odcizení médií nebo dokumentů	H3													0
							zneužití vnitřních prostředků (použití pro osobní účely, použití k jinému než legálnímu účelu), zneužití oprávnění	H4													0
							zneužití identity, falšování zpráv	H5													0
							zničení nebo poškození zařízení v důsledku změn prostředí (změny vlhkosti, teploty ale i přírodní katastrofy)	H6													0
							zneužití vyměnitelných technických nosičů dat a mobilních zařízení	H7													0
							poškození dat použitím aplikačních programů na špatná data z hlediska času	H8													0
							provedení neoprávněných činností, tj. činností k nimž uživatel nemá oprávnění	H9													0
							zneužití oprávnění ze strany uživatelů[5] a administrátorů	H10													0
							vzdálená špionáž	H11													0
							odposlech	H12													0
							cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	H13													0
							instalace zákeřného kódu	H14													0
							neoprávněné užití technického aktiva, tj. použití bez licence, použití nad rámec licence, použití bez oprávnění	H15													0
							dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky el. energie nebo jiných	H16													0
							přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	H17													0
							porušení bezpečnostní politiky	H18													0
							chybná identifikace technických aktiv	H19													0
						Personální aktiva	nedodržení smluvního závazku ze strany subdodavatele	H20													0
							pochybení ze strany zaměstnanců (včetně trestné činnosti)	H21													0
							nedostatečná odborná úroveň nebo bezpečnostní kvalifikace	H22													0
							přechod klíčového personálního aktiva ke konkurenci	H23													0
							vyzrazení informací	H24													0
							nedostatečné předání agendy / ztráta know-how při odchodu zaměstnance ze společnosti	H25													0
							chybná identifikace personálních aktiv	H26													0

POZNÁMKY POD ČAROU

1 Primárním aktivem je vždy služba, kterou zpracovává nebo poskytuje informační a komunikační systém.

2 Viz. návod pro vyplnění.

3 Hrozby, kterými jsou ohrožena daná aktiva, nikoli hrozby, jejichž aktéry jsou daná aktiva. Př. Zaměstnanci mohou být původci většiny hrozeb, které ohrožují technická aktiva.

4 Zahrnuje hrozby ohrožující fyzická média, data na nich uložená, jakož i dokumentu ve fyzické podobě.

5 Uživatelé zahrnují jak zaměstnance povinné osoby, tak jejích dodavatelů.

Návod pro vyplnění

Tento list obsahuje návod pro kategorizaci vyžadovanou při hodnocení rizika či určení okruhu bezpečnostní opatření.

OBSAH

HODNOCENÍ DŮLEŽITOSTI PODPŮRNÉHO AKTIVA

DŮVĚRNOST

Stupeň důležitosti	Definice	Vložit do tabulky
Nízká	Aktivum je veřejně přístupné nebo určeno ke zveřejnění. Narušení důvěrnosti neohrožuje zájmy povinné osoby a nebude mít negativní dopad.	1
Střední	Aktivum není veřejně přístupné a tvoří know-how povinné osoby. Jeho ochrana není vyžadována žádným právním předpisem ani smluvním ujednáním.	2
Vysoká	Aktivum není veřejně přístupné a tvoří know-how povinné osoby. Jeho ochrana je vyžadována právním předpisem nebo smluvním ujednáním (př. obchodní tajemství, osobní údaje).	3
Kritická	Aktivum není veřejně přístupné a vyžaduje nadstandardní míru ochrany nad rámec předchozí kategorie (př. strategické obchodní tajemství, zvláštní kategorie osobních údajů).	4

Zdroj: [2, příloha 1]

DOSTUPNOST

Stupeň důležitosti	Definice	Vložit do tabulky
Nízká	Narušení dostupnosti není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do1 týdne).	1
Střední	Narušení dostupnosti by nemělo překročit dobu 1 pracovního dne. Dlouhodobější výpadek může ohrozit oprávněné zájmy povinné osoby.	2
Vysoká	Narušení dostupnosti by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.	3
Kritická	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k závažnému ohrožení opráněných zájmů povinné osoby.	4

Zdroj: [2, příloha 1]

INTEGRITA

Stupeň důležitosti	Definice	Vložit do tabulky
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje zájmy povinné osoby.	1
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.	2
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.	3
Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.	4

Zdroj: [2, příloha 1]

HODNOCENÍ ZÁVAŽNOSTI HROZEB

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.	1
Střední	Hrozba je málo pravděpodobná až nepravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.	2
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.	3
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.	4

Zdroj: [2, příloha 2]

HODNOCENÍ DOPADU

BEZPEČNOST A ZDRAVÍ OSOB

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Žádné vodítko.	1
Střední	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) jedné nebo několika osob.	2
Vysoká	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) větší skupiny osob, nebo ohrožení na životě jednotlivců.	3
Kritická	Může vést k přímému ohrožení či ztrátě života skupiny osob.	4

Zdroj: [1, příloha 1]

MEZINÁRODNÍ VZTAHY

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Žádné vodítko.	1
Střední	Může vytvářet negativní obraz ČR v jednom teritoriu, popř. v 1 státě.	2
Vysoká	Může vytvářet negativní obraz ČR ve světě.	3
Kritická	Může negativně ovlivnit nebo poškodit diplomatické vztahy a tím způsobit nevýhodu pro zájmy ČR.	4

Zdroj: [1, příloha 1]

OCHRANA OSOBNÍCH ÚDAJŮ

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Může způsobit prušení interních předpisů a postupů, nikoli však porušení zákonných a smluvních povinností.	1
Střední	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).	2
Vysoká	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na jednotlivce (pokuta až 20 mil. EUR nebo 4% celkového ročního obratu - viz. čl. 83/5 GDPR).	3
Kritická	Žádné vodítko.	4

Zdroj: [1, příloha 1]

ŘÍZENÍ A PROVOZ ORGANIZACE

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Může narušit řádné řízení nebo fungování části nebo celé organizace.	1
Střední	Může omezit provádění důležitých činností organizace.	2
Vysoká	Může způsobit dočasné zastavení nebo podstatné narušení důležitých činností organizace nebo poškodit rozvoj nebo prosazování cílů a zájmů organizace.	3
Kritická	Závažným způsobem může zasáhnout do fungování celé organizace a může vést až k ukončení činnosti.	4

Zdroj: [1, příloha 1]

ZÁKONNÉ A SMLUVNÍ POVINNOSTI

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Může zapříčinit porušení interních předpisů a postupů, nikoli však k porušení zákonných a smluvních povinností.	1
Střední	Může zapříčinit správní nebo občanskoprávní řízení vedoucí k pokutě nebo náhradě škody.	2
Vysoká	Může zapříčinit porušení právních předpisů vedoucí k zahájení trestního stíhání.	3
Kritická	Žádné vodítko.	4

Zdroj: [1, příloha 1]

ZTRÁTA DŮVĚRYHODNOSTI

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Může negativně ovlivnit vztahy s jinými částmi organizace nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhého trvání.	1
Střední	Může negativně ovlivnit vztahy s jinými organizacemi nebo veřejností, negativní publicita se ale bude týkat omezené zájmové skupiny nebo bude široká, avšak krátkodobá.	2
Vysoká	Může závažně ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní negativní publicity.	3
Kritická	Může závažně a dlouhodobě ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní či nadnárodní negativní publicity, s dlouhodonými účinky a požadavky přijetí politické odpovědnosti.	4

Zdroj: [1, příloha 1]

TRESTNĚ-PRÁVNÍ ŘÍZENÍ

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Žádné vodítko.	1
Střední	Může vytvořit podmínky pro páchání trestné činnosti nebo může ztížit její vyšetřování.	2
Vysoká	Může vést k narušení vyšetřování trestné činnosti nebo soudnímu řízení (méně závažná kriminalita, krátkodobě, v jednotlivých případech).	3
Kritická	Může vést k závažnému dlohodobému narušení schopnosti vyšetřovat trestnou činnosti, popřípadě zpochybnění soudních řízení a rozhodnutí (závažná kriminalita, celkové zpochybnění systému).	4

Zdroj: [1, příloha 1]

FINANČNÍ ZTRÁTY

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Může přímo nebo nepřímo vést ke ztrátám menším než 0,05% ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	1
Střední	Může přímo nebo nepřímo vést ke ztrátám mezi 0,05% a 2% ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	2
Vysoká	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).	3
Kritická	Může přímo či nepřímo vést ke ztrátám přesahujícím 10% ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	4

Zdroj: [1, příloha 1]

VEŘEJNÝ POŘÁDEK

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Žádné vodítko.	1
Střední	Může zapříčinit rozsahem, formou nebo místem omezené protesty (lokální nepokoje).	2
Vysoká	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.	3
Kritická	Může zapříčinit hromadné nepokoje, např. generální stávku, nebo jinak závažně narušit pořádek s celostátními dopady.	4

Zdroj: [1, příloha 1]

ZAJIŠŤOVÁNÍ NEZBYTNÝCH SLUŽEB

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Žádné vodítko.	1
Střední	Může způsobit závažné omezení či narušení nezbytných služeb pro malé množství osob.	2
Vysoká	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.)	3
Kritická	Může způsobit rozsáhlé omezení poskytování nezbytných služeb nebo jiný závažný zásah do každodenního života postihující více než 125.000 osob.	4

Zdroj: [1, příloha 1]

HODNOCENÍ RIZIKA

Stupeň významnosti	Definice	Hodnota v tabulce
Nízké	Riziko je považováno za akceptovatelné.	1
Střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti je riziko akceptovatelné.	2
Vysoké	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.	3
Kritické	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.	4

Zdroj: [2, příloha 2]

HODNOCENÍ VÝZNAMU OPATŘENÍ

Stupeň významnosti	Definice	Hodnota v tabulce
Nízký	Význam opatření z hlediska předcházení realizace hrozby nebo snižování jejích dopadů je spíše podružný. V případě, že vyhodnocený stupeň rizika je 1 až 3, opatření není třeba implementovat.	1
Střední	Význam opatření z hlediska předcházení realizace hrozby nebo snižování jejích dopadů je střední. V případě, že vyhodnocený stupeň rizika je 1 nebo 2, opatření není třeba implementovat.	2
Vysoký	Význam opatření z hlediska předcházení realizace hrozby nebo snižování jejích dopadů je vysoký. V případě, že vyhodnocený stupeň rizika je 1, opatření není třeba implementovat.	3
Kritický	Opatření je třeba implementovat vždy, je považováno za minimální zabezpečení.	4
Podmíněný	Opatření je omezeno na specifické systémy či specifické situace, jeho aplikovatelnost je třeba vyhodnotit s přihlédnutím k hodnoceným aktivům a zvažovaným činnostem. Význam opatření nemůže být vyhodnocen v obecné rovině.	5

Zdroj: vlastní zpracování

TECHNICKÁ AKTIVA	DRUH OPATŘENÍ A JEHO VÝZNAM PRO PŘEDCHÁZENÍ ČI SNIŽOVÁNÍ DOPADŮ HROZBY																									
	ORGANIZAČNÍ OPATŘENÍ														TECHNICKÁ OPATŘENÍ											
HROZBA	Systém řízení bezpečnosti informací	Řízení aktiv	Řízení rizik	Organizační bezpečnost	Bezpečnostní role	Řízení dodavatelů	Bezpečnost lidských zdrojů	Řízení provozu a komunikací	Řízení změn	Řízení přístupu	Akvizice vývoj a údržba	Zvládání kybernetických bezpečnostních událostí a incidentů	Řízení kontinuity činností	Audit kybernetické bezpečnosti	Fyzická bezpečnost	Bezpečnost komunikačních sítí	Správa a ověřování identit	Řízení přístupových oprávnění	Ochrana před škodlivým kódem	Zaznamenávání událostí informačního a komunikačního systému	Detekce kybernetických bezpečnostních událostí	Sběr a vyhodnocování kybernetických bezpečnostních událostí	Aplikační bezpečnost	Kryptografické prostředky	Zajišťování úrovně dostupnosti informací	Průmyslové, řídící a obdobné systémy
porucha zařízení nebo chybné fungování aplikačního programového vybavení				2			2	4	3		5	3											1		2	5
nedbalostní nebo úmyslné poškození, chyba použití							4					2			3			3	3	2	2	2				5
ztráta, odcizení médií nebo dokumentů		2					4	2				3			3	1	4	4	3	3	3	3	1	2		5
zneužití vnitřních prostředků		4		4			4	5		3							3			2	2	2	1			
zneužití identity, falšování zpráv							4			4							4						2			
zničení nebo poškození zařízení v důsledku změn prostředí													3		4											
zneužití vyměnitelných technických nosičů dat		3					4			2									2							
poškození dat použitím aplikačních programů na špatná data z hlediska času																				4		4				
provedení neoprávněných činností, tj. provedení činností k nimž uživatel nemá oprávnění				4			4	4								1	4	3		2		2	2			5
zneužití oprávnění ze strany uživatelů a administrátorů				4			4	4		4								2								
vzdálená špionáž																3	4							2		
odposlech																4								2		
cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik		1					4			2						3	3									
instalace zákeřného kódu		1					4	4	5	1	5	2				3			4		2	2				
neoprávněné užití technického aktiva, tj. použití bez licence, použití nad rámec licence, použití bez oprávnění				4		4																				
dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb						4		4				3	3			2				3		3			3	5
přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie						4		4				2	2			2				2		2				5
porušení bezpečnostní politiky							4					1		1												
chybná identifikace technických aktiv	4																									

PERSONÁLNÍ AKTIVA	DRUH OPATŘENÍ A JEHO VÝZNAM Z HLEDISKA PŘEDCHÁZENÍ ČI SNIŽOVÁNÍ DOPADŮ HROZBY																									
	ORGANIZAČNÍ OPATŘENÍ														TECHNICKÁ OPATŘENÍ											
HROZBA	Systém řízení bezpečnosti informací	Řízení aktiv	Řízení rizik	Organizační bezpečnost	Bezpečnostní role	Řízení dodavatelů	Bezpečnost lidských zdrojů	Řízení provozu a komunikací	Řízení změn	Řízení přístupu	Akvizice vývoj a údržba	Zvládání kybernetických bezpečnostních událostí a incidentů	Řízení kontinuity činností	Audit kybernetické bezpečnosti	Fyzická bezpečnost	Bezpečnost komunikačních sítí	Správa a ověřování identit	Řízení přístupových oprávnění	Ochrana před škodlivým kódem	Zaznamenávání událostí informačního a komunikačního systému	Detekce kybernetických bezpečnostních událostí	Sběr a vyhodnocování kybernetických bezpečnostních událostí	Aplikační bezpečnost	Kryptografické prostředky	Zajišťování úrovně dostupnosti informací	Průmyslové, řídící a obdobné systémy
nedodržení smluvního závazku ze strany subdodavatele				3		4	3																			
pochybení ze strany zaměstnanců (včetně trestné činnosti)				4			4																			
nedostatečná odborná úroveň					2		4																			
přechod klíčového personálního aktiva ke konkurenci				4																						
vyzrazení informací				4			4	1																		
nedostatečné předání agendy / ztráta know-how při odchodu zaměstnance / dodavatele				4			4																			
chybná identifikace personálních aktiv	4																									

URČENÍ VÝZNAMNOSTI OPATŘENÍ - TECHNICKÁ AKTIVA

Na tomto listu je provedeno určení významnosti jednotlivých opatření stanovených VKB pro minimaliza

PRACOVNÍ METODIKA URČENÍ VÝZNAMNOSTI OPATŘENÍ

Kategorie opatření	Přiřazená vstupní hodnota
Preventivní opatření - podpůrné, omezená aplikovatelnost	1
preventivní opatření - méně významné	2
preventivní opatření - stěžejní	3
reaktivní opatření - stěžejní	3
reaktivní opatření - méně významné nebo omezená aplikovatelnost	2

Hrozba	Kategorie opatření	Dle mapovací tabulky
Porucha zařízení nebo chybné fungování aplikačního programového vybavení	Průmyslové, řídící a obdobné systémy	2
	Akvizice, vývoj a údržba	4
	Řízení provozu a komunikací	14
	Zvládní kybernetických událostí	5
	Řízení změn	10
	Zajišťování úrovně dostupnosti informací	3
	Organizační bezpečnost	3
	Bezpečnost lidských zdrojů	3
	Aplikační bezpečnost	1

nedbalostní nebo úmyslné poškození, chyba použití	Průmyslové, řídící a obdobé systémy	1
	Bezpečnost lidských zdrojů	6
	Fyzická bezpečnost	3
	Ochrana před škodlivým kódem	2
	Řízení přístupových oprávnění	3
	Bezpečnost komunikačních sítí	3
	Zvládání kybernetických událostí	3
	Řízení změn	2
ztráta, odcizení médií nebo dokumentů	Průmyslové, řídící a obdobné systémy	1
	Bezpečnost lidských zdrojů	15
	Správa a ověřování identit	
	Řízení přístupových oprávnění	6
	Ochrana před škodlivým kódem	3
	Fyzická bezpečnost	3
	Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	
	Kryptografické prostředky	2
	Řízení aktiv	3
	Řízení provozu a komunikací	7
	Bezpečnost komunikačních sítí	3

	Aplikační bezpečnost	1
	Zvládání kybernetických událostí	4
	Akvizice, vývoj a údržba	1
Zneužití vnitřních prostředků	Řízení provozu a komunikací	3
	Řízení aktiv	6
	Bezpečnost lidských zdrojů	15
	Organizační bezpečnost	3
	Správa a ověřování identit	
	Řízení přístupu	3
	Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	3
	Aplikační bezpečnost	1
	Akvizice, vývoj a údržba	1
zneužití identity, falšování zpráv	Bezpečnost lidských zdrojů	3
	Řízení přístupu	3
	Správa a ověřování identit	3
	Aplikační bezpečnost	3
Zničení nebo poškození zařízení v důsledku změn prostředí (změny vlhkosti, teploty ale i přírodní katastrofy)	Fyzická bezpečnost	3
	Řízení kontinuity činností	3
Zneužití vyměnitelných technických nosičů dat	Bezpečnost lidských zdrojů	6
	Řízení aktiv	5
	Ochrana před škodlivým kódem	3
	Řízení přístupu	3

poškození dat použitím aplikačních programů na špatná data z hlediska času	Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	3
Provedení neoprávněných činností, tj. provedení činností k nimž uživatel nemá oprávnění	Průmyslové, řídící a obdobné systémy	1
	Bezpečnost lidských zdrojů	9
	Správa a ověřování identit	3
	Organizační bezpečnost	3
	Řízení provozu a komunikací	3
	Řízení přístupových oprávnění	3
	Aplikační bezpečnost	3
	Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	3
	Bezpečnost komunikačních sítí	2
Zneužití oprávnění ze strany uživatelů a administrátorů, tj. provedení činností k nimž uživateli bylo uděleno oprávnění k jinému než zamýšlenému účelu	Organizační bezpečnost	2
	Řízení provozu a komunikací	2
	Řízení přístupu	3
	Bezpečnost lidských zdrojů	6
	Řízení přístupových oprávnění	2
Vzdálená špionáž	Správa a ověřování identit	3
	Bezpečnost komunikačních sítí	3
	Kryptografické prostředky	3
Odposlech	Bezpečnost komunikačních sítí	6
	Kryptografické prostředky	3

Cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	Bezpečnost lidských zdrojů	6
	Bezpečnost komunikačních sítí	6
	Správa a ověřování identit	3
	Řízení přístupu	3
	Řízení aktiv	2
Instalace zákeřného kódu	Akvizice, vývoj a údržba	1
	Řízení změn	1
	Ochrana před škodlivým kódem	3
	Řízení provozu a komunikací	2
	Bezpečnost lidských zdrojů	6
	Bezpečnost komunikačních sítí	5
	Zvládní kybernetických událostí	3
	Řízení aktiv	2
	Řízení přístupu	3
Neoprávněné užití technického aktiva, tj. použití bez licence, použití nad rámec licence, použití bez oprávnění	Řízení dodavatelů	3
	Organizační bezpečnost	6
dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	Průmyslové, řídící a obdobné systémy	2

	Řízení provozu a komunikací	5
	Řízení dodavatelů	3
	Zvládní kybernetických událostí	6
	Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	6
	Zajišťování úrovně dostupnosti informací	6
	Řízení kontinuity činností	3
	Bezpečnost komunikačních sítí	3
přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	Průmyslové, řídící a obdobné systémy	2
	Řízení dodavatelů	3
	Řízení provozu a komunikací	5
	Bezpečnost komunikačních sítí	3
	Zvládní kybernetických událostí	6
	Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	6
	Řízení kontinuity činností	3
porušení bezpečnostní politiky	Bezpečnost lidských zdrojů	6
	Zvládní kybernetických událostí	2
	Audit kybernetické bezpečnosti	2
chybná identifikace technických aktiv	Systém řízení bezpečnosti informací	3

ci naplnění hrozby, využití zranitelnosti či snížení dopadu.

Převod na stupnici 1-4	Výsledná hodnota, vč. korekce	Stručný popis
1	5	ochrana technického aktiv před využitím známých zranitelností a obnova chodu po kybernetickém bezpečnostním incidentu - omezeno na průmyslové, řídící a obdobné specifické systémy
1	5	řízení významných změn v souvislosti s plánovanou akvizicí a údržbou, zahrnutí bezpečnostních požadavků do projektu, provádění bezpečností testování před jejich zavedením do provozu
4	4	stanovení práv a povinností administrátorů a uživatelů, řízení tech. zranitelností, řízení a schvalování provozních změn, sledování a plánování kapacity lidských a technických zdrojů, zajištění kontaktu na osoby systémové a technické podpory
2	3	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
3	3	přezkoumávání možných dopadů změny, určení významných změn, rozhodntí o provedení testování zranitelností
1	2	zajištění dostupnosti a redundance technických aktiv nezbytných pro provoz informačního a komunikačního systému, a to s ohledem na hodnocení podpůrných aktiv
1	2	zajištění dostupnosti zdrojů, dostatečné pravomoci a zdroje k požadované údržbě, dostatečné interní priority
1	2	bezpečnostní školení administrátorů, osob zastávajících bezpečnostní role a dodavatelů
1	1	penetrační testy před uvedením významné změny do provozu - omezeno na důležitá aktiva a význmané změny

1	5	omezení fyzického přístupu k zařízením průmyslových, řídících a obdobných specifických systémů; vyčlenění komunikační sítě určené pro průmyslové, řídící a obdobné specifické systémy od ostatní infrastruktury
4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní, stanovení pravidel a postupů pro řešení případů bezpečnostních pravidel uživateli
2	3	předchází poškození, krádeži nebo zneužití aktiv
1	3	nasazení nástroje pro nepřetržitou automatickou ochranu, řízení oprávnění ke spouštění kódu, řízení automatického spouštění obsahu výměnných zařízení a datových nosičů
2	3	řízení přístupu k informačnímu a komunikačnímu systému a přijetí opatření, která slouží k zajištění ochrany a obrana proti zneužití
2	2	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
2	2	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
1	0	není relevantní
1	5	omezení fyzického přístupu k zařízením průmyslových, řídících a obdobných specifických systémů
4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní; pravidla a postupy pro řešení případů bezpečnostních pravidel uživateli
	4	nasazení nástroje pro správu a ověření identity uživatelů, autentizační mechanismus
2	4	řízení přístupu k jednotlivým aktivům
1	3	nasazení nástroje pro nepřetržitou automatizovanou ochranu před škodlivým kódem a jeho pravidelná aktualizace; nasazováno s ohledem na důležitost aktiv
1	3	předcházení poškození, krádeži, zneužití aktiva nebo přerušení poskytování služeb, stanovení fyzického bezpečnostního perimetru
	3	zaznamenávání bezpečnostních a potřebných provozních událostí důležitých aktiv
1	2	použití aktuálně odolných kryptografických algoritmů a klíčů
1	2	určení způsobu likvidace dat, provozních údajů, informací a jejich kopií nebo likvidace technických nosičů
2	2	oddělení vývojového, testovacího a provozního prostředí, provádění pravidelných záloh, zajištění bezpečnosti informací v průběhu celého životního cyklu
1	1	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě

1	1	trvalá ochrana aplikací, informací a transakcí před neoprávněnou činností a popřením provedených činností
1	1	proces detekce kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů
1	0	není relevantní
1	5	oddělení vývojového, testovacího a provozního prostředí
2	4	stanovení přípustných způsobů používání aktiva, určení způsobu likvidace dat, provozních údajů, informací a jejich technických nosičů
4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní, kontrola dodržování bezpečnostní politiky uživateli
1	4	zajištění, aby byla zachovávána mlčenlivost administrátorů a osob zastávajících bezpečnostní role
	3	nasazení nástroje pro správu a ověření identity uživatelů, autentizační mechanismus
1	3	řízení přístupu k jednotlivým aktivům
1	2	zaznamenávání bezpečnostních a potřebných provozních událostí důležitých aktiv
1	1	trvalá ochrana aplikací, informací a transakcí před neoprávněnou činností a popřením provedených činností
1	0	oddělení vývojového, testovacího a provozního prostředí
4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní, kontrola dodržování bezpečnostní politiky uživateli
4	4	odebrání nebo změna přístupových oprávnění při změně pozice, zařazení, změně smluvního vztahu
4	4	nasazení nástroje pro správu a ověření identity uživatelů, autentizační mechanismus
4	2	trvalá ochrana aplikací, informací a transakcí před neoprávněnou činností
4	4	předcházení poškození, krádeži, zneužití aktiva nebo přerušení poskytování služeb, stanovení fyzického bezpečnostního perimetru
4	3	havarijní plány
4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní, kontrola dodržování bezpečnostní politiky uživateli
3	3	určení způsobu likvidace technických nosičů dat s ohledem na úroveň aktiv, určení přípustného způsobu používání aktiva
2	2	monitoring používání výměnných zařízení a datových nosičů
2	2	stanovení bezpečnostních opatření pro používání mobilních zařízení a jiných technických zařízení, kt. povinná osoba nemá ve své správě

3	4	zajištění synchronizace jednotného čassu technických aktiv nejméně jednou za 24h
1	5	omezení vzdáleného přístupu k těmto systémům
4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní, kontrola dodržování bezpečnostní politiky uživateli
1	4	nasazení nástroje pro správu a ověření identity uživatelů, autentizační mechanismus
1	4	stanovení pravidel pro určení administrátorů
1	4	stanovení práv a povinností administrátorů, uživatelů a osob zastávajících bezpečnostní role
1	3	použití centralizovaného nástroje pro řízení přístupových oprávnění k aktivům
1	2	ochrana aplikací, informací a transakcí před neoprávněnou činností
1	2	zaznamenávání bezpečnostních a potřebných provozních údálostí důležitých aktiv
1	1	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
1	4	stanovení pravidel pro určení administrátorů
1	4	stanovení práv a povinností administrátorů, uživatelů a osob zastávajících bezpečnostní role
2	4	odebrání nebo změna přístupových oprávnění při ukončení nebo změně smluvního vztahu nebo pozice
4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní, kontrola dodržování bezpečnostní politiky uživateli
1	2	použití centralizovaného nástroje pro řízení přístupových oprávnění k aktivům
4	4	zajištění odolnosti uložených a přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití, vynucování minimálních standardů pro tvorbu hesla
4	3	segmentace stě, řízení komunikace v rámci sítě, kryptografie, blokace nežádoucí komunikace, využití nástroje pro ochranu integrity komunikační sítě
4	2	použití aktuálně odolných kryptografických algoritmů a klíčů
4	4	segmentace stě, řízení komunikace v rámci sítě, kryptografie, blokace nežádoucí komunikace, využití nástroje pro ochranu integrity komunikační sítě
2	2	použití aktuálně odolných kryptografických algoritmů a klíčů

4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní, kontrola dodržování bezpečnostní politiky uživateli
4	3	aktivní blokace nežádoucí komunikace
2	3	zajištění odolnosti uložených a přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití, vynucování minimálních standardů pro tvorbu hesla
2	2	omezení a kontrola používání programových prostředků schopných překonat systémové nebo aplikační kontroly
1	1	stanovení přípusných způsobů používání aktiv, a pravidla manipulace s aktivy s ohledem na úroveň aktiv
1	5	stavenovení požadavků na technické aktivum v projektu akvizice, vývoje a údržby
1	5	provádění analýzy rizik, přijetí opatření za účelem snížení nepříznivých dopadů změny
2	4	použití nástroje pro nepřetržitou automatizovanou ochranu před škodlivým kódem a jeho pravidelná aktualizace - nasazováno s ohledem na důležitost aktiv
1	4	pravidla a postupy pro zajištění bezpečnosti síťových služeb, pravidla a postupy pro ochranu před škodlivým kódem
4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní, kontrola dodržování bezpečnostní politiky uživateli
3	3	segmentace stě, řízení komunikace v rámci sítě, kryptografie, blokace nežádoucí komunikace, využití nástroje pro ochranu integrity komunikační sítě
2	2	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
1	1	stanovení přípusných způsobů používání aktiva a pravidel manipulace s aktivy s ohledem na úroveň aktiv
2	1	omezení a kontrola používání programových prostředků schopných překonat systémové nebo aplikační kontroly
2	4	implementace pravidel dle přílohy 7 VKB, písm. b) - oprávnění užívat data, c) - autorství programového kódu; požadevek dle písm. f) jsou omezeny na významné dodavatele; předpokladem je stanovení garanta aktiva a udělení dostaečných pravomocí a zdrojů k pořízení licence
4	4	zajištění integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu akvizice předmětů chráněných duševním vlastnictvím
1	5	ochrana tech. aktiv před využitím známých zranitelností a obnova chodu po kybernetickém bezp. incidentu, vyčlenění od ostatní infastruktury - omezeno na průmyslové, řídící a obdobné specifické systémy

3	4	postupy pro sledování kybernetických bezpečnostních událostí, zajištění spojení na kontaktní osoby pověřené výkonem systémové a technické podpory
2	4	stanovení pravidel pro dodavatele a jejich pravidelné přezkoumávání, u významných též dle přílohy 7 VKB písm. k) - specifikace podmínek pro řízení kontinuity činností
4	3	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
4	3	zaznamenávání bezpečnostních a potřebných provozních údálostí důležitých aktiv
4	3	zajištění dostupnosti a redundance tech. aktiv nezbytných pro provoz informačního a komunikačního systému a to s ohledem na hodnocení podpůrných aktiv.
2	3	plány kontinuity činností
2	2	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
1	5	ochrana technických aktiv před využitím známých zranitelností a obnova chodu po kybernetickém bezpečnostním incidentu, vyčlenění od ostatní infastruktury - omezeno na průmyslové, řídící a obdobné specifické systémy
2	4	stanovení pravidel pro dodavatele a jejich pravidelné přezkoumávání, u významných též dle přílohy 7 písm. k) - specifikace podmínek pro řízení kontinuity činností
3	4	postupy pro sledování kybernetických bezpečnostních událostí, Zajištění spojení na kontaktní osoby pověřené výkonem systémové a technické podpory
2	2	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
4	2	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
4	2	zaznamenávání bezpečnostních a potřebných provozních údálostí důležitých aktiv
2	2	plány kontinuity činností
4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní, kontrola dodržování bezpečnostní politiky ze strany uživatelů
1	1	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
1	1	pravidelný audit kybernetické bezpečnosti
4	4	určení organizačních částí a aktiv, kterých se systém řízení bezpečnosti týká

URČENÍ VÝZNAMNOSTI OPATŘENÍ- PERSONÁLNÍ AKTIVA

Na tomto listu je provedeno určení významnosti jednotlivých opatření stanovených VKB pro minimalizac

PRACOVNÍ METODIKA URČENÍ VÝZNAMNOSTI OPATŘENÍ

Kategorie opatření	Přiřazená vstupní hodnota
Preventivní opatření - podpůrné, omezená aplikovatelnost	1
preventivní opatření - méně významné	2
preventivní opatření - stěžejní	3
reaktivní opatření - stěžejní	3
reaktivní opatření - méně významné nebo omezená aplikovatelnost	2

Hrozba	Kategorie opatření	Dle mapovací tabulky
nedodržení smluvního závazku ze strany subdodavatele	Řízení dodavatelů	8
	Organizační bezpečnost	3
	Bezpečnost lidských zdrojů	6
pochybení ze strany zaměstnanců (včetně trestné činnosti)	Bezpečnost lidských zdrojů	9
	Organizační bezpečnost	4
nedostatečná odborná úroveň	Bezpečnost lidských zdrojů	6
	Bezpečnostní role	2
přechod klíčového personálního aktiva ke konkurenci	Organizační bezpečnost	4

vyzrazení informací	Organizační bezpečnost	3
	Bezpečnost lidských zdrojů	6
	Řízení provozu a komunikací	2
nedostatečné předání agendy nebo ztráta know-how při odchodu zaměstnance nebo dodavatele	Bezpečnost lidských zdrojů	3
	Organizační bezpečnost	3
chybná identifikace personálních aktiv	Systém řízení bezpečnosti informací	3

:i naplnění hrozby, využití zranitelnosti či snížení dopadu.

Převod na stupnici 1-4	Výsledná hodnota, vč. korekce	Stručný popis
4	4	hodnocení rizik v rámci výběrového řízení - omezeno na významné dodavatele, stanovení pravidel pro dodavatele, seznámení dodavatele s pravidly, u významných stanovení způsobů a urovní realizace bezpečnostních oprávnění a rozsah vzájemné smluvní odpovědnosti
2	3	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu výběru dodavatelů
3	3	poučení dodavatelů, pravidelné školení a ověřování bezpečnostního povědomí, kontrolu dodržování bezpečnostní politiky uživateli
4	4	poučení dodavatelů, pravidelné školení a ověřování bezpečnostního povědomí, kontrolu dodržování bezpečnostní politiky uživateli
2	4	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu výběru zaměstnanců a stanovení pracovních nápní zaměstnanců
4	4	pravidelné školení a ověřování bezpečnostního povědomí zamětnanců v souladu s jejich pracovní náplní
1	2	dodržení minimální předepsané úrovně odbornosti - stanoveno pouze pro základní bezpečnostní role, nikoli celou organizační strukturu
4	4	integraci systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu vyjednávání a uzavírání pracovních smluv

2	4	zajištění, aby byla zachovávána mlčenlivost administrátorů a osob zastávajících bezp. role. - vztahuje se pouze na vybrané skupiny
4	4	poučení dodavatelů, pravidelné školení a ověřování bezpečnostního povědomí, kontrolu dodržování bezpečnostní politiky uživateli
1	1	pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu
4	4	zajištění, aby v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role byla předána odpovědnost - omezeno na vybrané skupiny
4	4	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu odchodu zaměstnance nebo dodavatele
4	4	určení organizačních částí a aktiv, kterých se systém řízení bezpečnosti týká

MAPOVACÍ TABULKA

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H1	zastaralost a nedostatečná údržba technického aktiva	Řízení změn	§11(1)(3)	**Řízení aktiv** §4, odst. 1, písm. f), g), opatření dle §4 odst. 1, písm. a) až e) jsou další prerekvizity	přezkoumávání dopadu změny, rozhodnutí o penetračním testování, testování zranitelností
porucha zařízení nebo chybné fungování aplikačního programového vybavení		Akvizice, vývoj a údržba	§13(f)	**Akvizice, vývoj a údržba** §13, písm. a), b), c), **Řízení změn** §11	bezpečnostní testování významných změn před uvedením do provozu, zákon požaduje jen u významných změn
		Organizační bezpečnost	§6(1)(c)(k)(g)	**Organizační bezpečnost** §6(3)(b - architekt KB), (c-garant aktiva), **Systém řízení bezpečnosti informací** §3	dostupnost zdrojů, dostatečné pravomoci nebo zdroje k požadované údržbě, dostatečná interní priorita
		Řízení provozu a komunikací	§10(1)(a)(e)(h)(f)	**Řízení aktiv, Řízení rizik, Organizační opatření** (metodiky chování uživatelů, definování komunikací)	řízení tech. zranitelnostní, sledování, plánování a řízení kapacity technického aktiva
		Řízení provozu a komunikací	§10(1)(b)	§15 **Řízení kontinuity činností**	pravidla spouštění, restartu systému, ošetření chybových stavů a mimořádných jevů; postup a zodpovědnosti dle plánu kontinuity činností či interních směrnic
		Zvládní kybernetických událostí	§14(1)	§22-24 **Zaznamenávání událostí informačního systému**, §9 **Bezpečnost lidských zdrojů** - odst. 1, písm. a), c), d),e), h)	automatizovaný proces detekce kybernetických bezp. událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
		Zajišťování úrovně dostupnosti informací	§27	§15 **Řízení kontinuity činností**, **Řízení aktiv** §4, odst. 1, písm. f), g), opatření dle §4 odst. 1, písm. a) až e) jsou další prerekvizity, **Řízení prozovu a komunikací**	zajištění dostupnosti a redundance technických aktiv nezbytných pro provoz informačního a komunikačního systému, a to s ohledem na hodnocení podp. aktiv
		Průmyslové, řídící a obdobné systémy	§28 (e)(f)	**Řízení aktiv** §4, **Řízení rizik** §5	ochrana technických aktiv před využitím známých zranitelností a obnova chodu po kybernetickém bezpečnostním incidentu - omezeno na průmyslové, řídící a obdobné specifické systémy
	nesprávná konfigurace technického aktiva	Řízení provozu a komunikací	§10(1)(a)(j)(g)	**Bezpečnost lidských zdrojů** §9(1)(a)(c)	pravidla a postupy pro instalaci technických aktiv a postupy řízení a schvalování provozních změn
		Bezpečnost lidských zdrojů	§9(1)(c)	opatření dle písm. a) a b)	bezpečnostní školení administrátorů, osob zastávajících bezpečnostní role a dodavatelů
		Akvizice, vývoj a údržba	§13(f)	opatření dle §13, písm. a), b), c)	bezpečnostní testování významných změn před uvedením do provozu, zákon požaduje jen u významných změn
		Řízení změn	§11(1)(3)	**Řízení aktiv** §4, odst. 1, písm. f), g), opatření dle §4 odst. 1, písm. a) až e) jsou další prerekvizity	přezkoumávání dopadu změny, rozhodnutí o penetračním testování, testování zranitelností
		Zvládní kybernetických událostí	§14(1)	§22-24 **Zaznamenávání událostí informačního systému**, §9 **Bezpečnost lidských zdrojů** - odst. 1, písm. a), c), d),e), h)	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
	nejasné nebo neúplné zadání pro vývojáře, neodladěný nebo nový program	Akvizice, vývoj a údržba	§13(c)(d)(f)	**Systém řízení bezpečnosti informací** §3(b), Řízení aktiv §4(1)(h), **Řízení rizik** §5, **Řízení změn** §11	stanovení bezpečnostních požadavků a jejich zahrnutí do projektu vývoje a údržby informačního a komunikačního systému
		Řízení změn	§11	**Řízení aktiv** §4, odst. 1, písm. f), g), opatření dle §4 odst. 1, písm. a) až e) jsou další prerekvizity, **Organizační bezpečnost** §6, odst. 1, písm. c), k), g), §6(3)(b - architekt KB), na to navazuje **Bezpečnost lidských zdrojů** §9(1)(d)	přezkoumávání dopadu změny, rozhodnutí o penetračním testování, testování zranitelností
	žádné nebo nedostatečné testování programů	Aplikační bezpečnost	§25(1)	**Řízení změn** §11(1), **Řízení provozu a komunikací** §10(1)(g), **Řízení aktiv** §4	provádění penetračních testů se zaměřením na důležitá aktiva
		Řízení provozu a komunikací	§10(1)(a)(g)	**Řízení aktiva** §4, **Řízení rizik** §5	postupy řízení a schvalování provozních změn
	použití nevhodného nebo nekompatibilního technického aktiva (př. aktiva obsahujícího známé chyby)	**Řízení změn**	§11(1)	**Řízení aktiv** §4, odst. 1, písm. f), g), opatření dle §4 odst. 1, písm. a) až e) jsou další prerekvizity, **Organizační bezpečnost** §6, odst. 1, písm. c), k), g), §6(3)(b - architekt KB), na to navazuje **Bezpečnost lidských zdrojů** §9(1)(d)	přezkoumávání dopadu změny, u významných změn též provedení analýzy rizik
		Řízení provozu a komunikací	§10(1)(e)(g)	**Řízení změn** §11(1)	řízení technických zranitelností, schvalování provozních změn
		Průmyslové, řídící a obdobné systémy	§28(a)	**Řízení aktiv** §4, **Řízení rizik** §5	použití technických a programových prostředků určených do specifického prostředí - omezeno na průmyslové, řídící a obdobné specifiké systémy
		Akvizice, vývoj a údržba	§13(d)	**Systém řízení bezpečnosti informací** §3(b), Řízení aktiv §4(1)(h), **Řízení rizik** §5, **Řízení změn** §11	stavenovení požadavků na technické aktivum v projektu akvizice, vývoje a údržby, zákon vyžaduje pouze u významných změn

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H2	nedostatečná ochrana vnějšího perimetru, nesprávné uskladnění	**Fyzická bezpečnost**	§17(a)(c)	**Systém řízení bezpečnosti informací** §3, §17(b)	předcházení poškození, krádeži, zneužití aktiva nebo přerušení poskytování služeb, stanovení fyzického bezpečnostního perimetru
nedbalostní nebo úmyslné poškození, chyba použití		Ochrana před škodlivým kódem		§4(1)(h) - **Řízení aktiv,** odst. 1, písm. a) až g) jsou další podpůrná opatření	použití nástroje pro nepřetržitou automatizovanou ochranu před škodlivým kódem a jeho pravidelná aktualizace; nasazováno s ohledem na důležitost aktiv
		Bezpečnost komunikačních sítí	§18(a)(b)(d)(e)	§4(1)(h) - **Řízení aktiv,** odst. 1, písm. a) až g) jsou další podpůrná opatření	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
		Průmyslové, řídící a obdobé systémy	§28(b)(c)	**Řízení aktiv** §4, **Řízení rizik** §5	omezení fyzického přístupu k zařízením průmyslových, řídících a obdobných specifických systémů; vyčlenění komunikační sítě určené pro průmyslové, řídící a obdobné specifické systémy od ostatní infrastruktury
		Řízení přístupových oprávnění	§12(1)	**Systém řízení bezpečnosti informací** §3, **Řízení aktiv** §4(1)(a)-(i), **Správa a ověřování identit** §19, **Řízení přístupových oprávnění** §20	řízení přístupu k jednotlivým aktivům
		Zvládání kybernetických událostí	§14(1)	§22-24 **Zaznamenávání událostí informačního systému**, §9 **Bezpečnost lidských zdrojů** - odst. 1, písm. a), c), d),e), h)	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
	nedostatečné bezpečnostní povědomí uživatelů a nesprávná manipulace	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní; předpokladem opatření jsou opatření v oblasti Bezpečnosti lidských zdrojů, ustanovení potřebných bezpečnostních rolí a Řízení provozu a komunikací
		Bezpečnost lidských zdrojů	§9(1) (i)	Bezpečnost lidských zdrojů - §9, odst. 1, písm. c), e)	pravidla a postupy pro řešení případů bezpečnostních pravidel uživateli
	složité uživatelské rozhraní, nedostatečná dokumentace	Řízení změn	§11	**Řízení aktiv** §4, odst. 1, písm. f), g), opatření dle §4 odst. 1, písm. a) až e) jsou další prerekvizity.	přezkoumávání možných odpadů změny, funkční a nefunkční požadavky jsou zvažovány v širším kontextu hodnocení změny; hodnocení rizika změny je zákonem požadováno pouze u významných změn
		Bezpečnost lidských zdrojů	§9(1)(e)	**Organizační bezpečnost** §6	pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H3	nedostatečná ochrana perimetru - fyzického i virtuálního, nesprávné uskladnění	**Fyzická bezpečnost**	§17(a)(c)	§17(b), §4(1)(h) - **Řízení aktiv**, odst. 1, písm. a) až g) jsou další podpůrná opatření	předcházení poškození, krádeži, zneužití aktiva nebo přerušení poskytování služeb, stanovení fyzického bezpečnostního perimetru
		Průmyslové, řídící a obdobné systémy	§28(b)	§4(1)(h) - **Řízení aktiv**, odst. 1, písm. a) až g) jsou další podpůrná opatření	omezení fyzického přístupu k zařízením průmyslových, řídících a obdobných specifických systémů
		Řízení přístupových oprávnění	§12(1)	**Systém řízení bezpečnosti informací** §3, **Řízení aktiv** §4(1)(a)-(i), **Správa a ověřování identit** §19, **Řízení přístupových oprávnění** §20	řízení přístupu k jednotlivým aktivům
		Správa a ověřování identit	§19	**Řízení přístupu** §12, **Řízení aktiv** §4	nasazení nástroje pro správu a ověření identity uživatelů, autentizační mechanismus
		Bezpečnost lidských zdrojů	§9(1)(a)(c)(e)	**Systém řízení bezpečnosti informací** §3	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní
		Ochrana před škodlivým kódem	§21(1)(a)(e)	§4(1)(h) - **Řízení aktiv,** odst. 1, písm. a) až g) jsou další podpůrná opatření	nasazení nástroje pro nepřetržitou automatizovanou ochranu před škodlivým kódem a jeho pravidelná aktualizace - nasazováno s ohledem naůdležitost aktiv
		Kryptografické prostředky	§26	**Řízení aktiv** §4(1)(i), S**ystém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(l), **Bezpečnost komunikačních sítí** §18	použití aktuálně odolných kryptografických algoritmů a klíčů
		Bezpečnost komunikačních sítí	§18(a)(b)(d)(e)	§4(1)(h) - **Řízení aktiv,** odst. 1, písm. a) až g) jsou další podpůrná opatření	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
		Aplikační bezpečnost	§25(2)	**Řízení přístupu** §12, **Systém řízení bezpečnosti informací** §3, **Řízení aktiv** §4(1)(a)-(i), **Bezpečnostní role** §7(3), **Správa a ověřování identit** §19, **Řízení přístupových oprávnění** §20	trvalá ochrana aplikací, informací a transakcí před neoprávněnou činností a popřením provedených činností
		Zvládání kybernetických událostí	§14(1)	§22-24 **Zaznamenávání událostí informačního systému**, §9 **Bezpečnost lidských zdrojů** - odst. 1, písm. a), c), d),e), h)	proces detekce kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů
	nedostatečné postupy likvidace	**Řízení aktiv**	§4(1)(j)	**Řízení aktiv** §4 odst. 1, písm. a) až g), §3 **Systém řízení bezpečnosti informací** §3	určení způsobu likvidace dat, provozních údajů, informací a jejich kopií nebo likvidace technických nosičů
	nekontrolované kopírování	Řízení provozu a komunikací	§10(1)(a)(i)	**Řízení aktiv** §4 odst. 1, písm. a) až g)	stanovení pravidel a postupů pro ochranu informací a dat v průběhu celého životního cyklu
		Bezpečnost lidských zdrojů	§9(1)(a)(c)(e)	**Systém řízení bezpečnosti informací** §3	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní
		Bezpečnost lidských zdrojů	§9(1)(i)	**Bezpečnost lidských zdrojů** - §9, odst. 1, písm. c), e)	pravidla a postupy pro řešení případů bezpečnostních pravidel uživateli
	nedostatečné bezpečnostní povědomí uživatelů (př. nedostatečné dodržování pravidel prázdného stolu a prázdné obrazovky monitoru)	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní; předpokladem opatření jsou opatření v oblasti Bezpečnosti lidských zdrojů, ustanovení potřebných bezpečnostních rolí a Řízení provozu a komunikací
	nedostatečné monitorování činnosti uživatelů a neschopnost odhalit jejich nevhodné a závadné způsoby chování (př. nedostatečná kontrola práce externích zaměstnanců nebo	**Bezpečnost lidských zdrojů**	§9(1)(i)	**Systém řízení bezpečnosti informací** §3, **Bezpečnost lidských zdrojů** - §9, odst. 1, písm. c), e)	pravidla a postupy pro řešení případů bezpečnostních pravidel uživateli
		Zvládání kybernetických událostí	§14(1)	**Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů** §22 odst.1, písm. a)	proces detekce kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů
	nedostatečný proces zálohování dat	**Řízení provozu a komunikací**	§10(1)(k)	§15 **Řízení kontinuity činností**, písm. b), bod 3	provádění pravidelného zálohování a kontroly použitelnosti provedených záloh
	nedostatečný schvalovací proces prostředků pro zpracování informací	**Řízení přístupových oprávnění**	§12(1)	**Systém řízení bezpečnosti informací** §3, **Řízení aktiv** §4(1)(a)-(i), **Bezpečnostní role** §7(3), **Správa a ověřování identit** §19, **Řízení přístupových oprávnění** §20	řízení přístupu k jednotlivým aktivům
		Bezpečnost lidských zdrojů	§9(1)(i)	**Organizační bezpečnost** §6	stanovení pravidel a postupů pro řešení případů porušení
	nedostatečná ochrana dat v testovacím a/nebo vývojovém prostředí	**Řízení provozu a komunikací**	§10(3)	**Řízení aktiv** §4(1)(i)	oddělení vývojového, testovacího a provozního prostředí
		Akvizice, vývoj a údržba	§13(e)	**Systém řízení bezpečnosti informací** §3(b), Řízení aktiv §4(1)(h), **Řízení rizik** §5, **Řízení změn** §11	zajištění bezpečnost vývojového a testevacího prostředí a ochrany používaných testovacích dat

ztráta, odcizení médií nebo dokumentů

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H4	nedostatečně či nevhodně stanovené přípustné způsoby užívání a manipulace s technickým aktivem	**Řízení aktiv**	§4(1)(i)	**Řízení aktiv** §4 odst. 1, písm. a) až g), **Systém řízení bezpečnosti informací** §3, **Bezpečnostní role** §7(3)	stanovení přípustných způsobů používání aktiva
zneužití vnitřních prostředků (např. použití pro osobní účely, použití k jinému než legálnímu účelu)	nedostatečné školení uživatelů a kontrola dodržování ze strany managementu	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)(f)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení uživatelu, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní; zajištění kontroly dodržování bezpečnostní politiky ze strany uživatelů; předpokladem opatření jsou opatření v oblasti Bezpečnosti lidských zdrojů, ustanovení potřebných bezpečnostních rolí a Řízení provozu a komunikací
		Bezpečnost lidských zdrojů	§9(1)(i)	**Bezpečnost lidských zdrojů** - §9, odst. 1, písm. c), e)	pravidla a postupy pro řešení případů bezpečnostních pravidel uživateli
	nedostatečné monitorování činnosti uživatelů a neschopnost odhalit jejich nevhodné a závadné způsoby chování (vč. neprovádění logování, nedostatečné postupy pro zjištění bezpečnostních slabin)	**Bezpečnost lidských zdrojů**	§9(1)(i)	**Systém řízení bezpečnosti informací** §3**, Bezpečnost lidských zdrojů** - §9, odst. 1, písm. c), e)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
		Aplikační bezpečnost	§25(2)	**Řízení přístupu** §12, **Systém řízení bezpečnosti informací** §3, **Řízení aktiv** §4(1)(a)-(i), **Bezpečnostní role** §7(3), **Správa a ověřování identit** §19, **Řízení přístupových oprávnění** §20	trvalá ochrana aplikací, informací a transakcí před neoprávněnou činností a popřením provedených činností
		Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	§22	**Řízení aktiv** §4	zaznamenávání bezpečnostních a potřebných provozních událostí důležitých aktiv
	vyřazení nebo opětovné použití záznamových médií bez důkladného vymazání	**Řízení aktiv**	§4(1)(j)	**Systém řízení bezpečnosti informací** §3, **Řízení aktiv** §4 odst. 1, písm. a) až g)	určení způsobu likvidace dat, provozních údajů, informací a jejich technických nosičů
	chybné přiřazení přístupových práv	**Řízení přístupu**	§12(1)(2)	**Systém řízení bezpečnosti informací** §3, **Řízení aktiv** §4(1)(a)-(i), **Bezpečnostní role** §7(3), **Správa a ověřování identit** §19, **Řízení přístupových oprávnění** §20	řízení přístupu k jednotlivým aktivům
	nedostatečné postupy při identifikaci uživatele	**Správa a ověřování identit**	§19	**Řízení přístupu** §12, **Řízení aktiv** §4	nasazení nástroje pro správu a ověření identity uživatelů, autentizační mechanismus
	použití produkčních dat ve vývojovém a/nebo testovacím prostředí	**Řízení provozu a komunikací**	§10(3)	**Řízení aktiva** §4	oddělení vývojového, testovacího a provozního prostředí
		Akvizice, vývoj a údržba	§13(e)	**Systém řízení bezpečnosti informací** §3(b), Řízení aktiv §4(1)(h), **Řízení rizik** §5, **Řízení změn** §11	zajištění bezpečnosti vývojového a testovacího prostředí a ochrany používaných testovacích dat
	porušení mlčenlivosti uživatelů (smluvní nebo zákonné)	**Organizační bezpečnost**	§6(1)(j)	**Systém řízení bezpečnosti informací** §3	zajištění, aby byla zachovávána mlčenlivost administrátorů a osob zastávajících bezpečnostní role
		Bezpečnost lidských zdrojů	§9(1)(c)(e)(h)(f)	**Systém řízení bezpečnosti informací** §3**, Bezpečnost lidských zdrojů** §9 opatření dle písm. a) a b)	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní; zajištění kontroly dodržování bezpečnostní politiky ze strany uživatelů; předpokladem opatření jsou opatření v oblasti Bezpečnosti lidských zdrojů, ustanovení potřebných bezpečnostních rolí a Řízení provozu a komunikací
		Bezpečnost lidských zdrojů	§9(1)(i)	**Bezpečnost lidských zdrojů** - §9, odst. 1, písm. c), e)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H5	nedostatečná identifikace a autentizace, např. autentizace uživatele, nechráněné tabulky s hesly, špatná správa hesel	**Aplikační bezpečnost**	§25(2)(a)	**Řízení přístupu** §12, **Systém řízení bezpečnosti informací** §3, **Řízení aktiv** §4(1)(a)-(i), **Bezpečnostní role** §7(3), **Správa a ověřování identit** §19, **Řízení přístupových oprávnění** §20	trvalá ochrana aplikací, informací a transakcí před neoprávněnou činností
zneužití identity	nedostatečné postupy při identifikaci uživatele	**Správa a ověřování identit**	§19	**Řízení přístupu** §12, **Řízení aktiv** §4	nasazení nástroje pro správu a ověření identity uživatelů, autentizační mechanismus
	neodhlášení se při opuštění pracovní stanice	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)(f)	**Systém řízení bezpečnosti informací** §3, **Bezpečnost lidských zdrojů** §9 opatření dle písm. a) a b)	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní; zajištění kontroly dodržování bezpečnostní politiky ze strany uživatelů
	neodebrání přístupu při skončení zaměstnání / změně pozice	**Řízení přístupu**	§12(2)(m)(l)	§20(a) **Řízení přístupových oprávnění**	odebrání nebo změna přístupových oprávnění při změně pozice, zařazení, změně smluvného vztahu
H6	nedostatečná ochrana vnějšího perimetru (př. poloha v záplavové oblasti; prašné, vlhké prostředí)	**Fyzická bezpečnost**	§17(a)(c)	§17(b), §4(1)(h) - **Řízení aktiv**, odst. 1, písm. a) až g) jsou další podpůrná opatření	předcházení poškození, krádeži, zneužití aktiva nebo přerušení poskytování služeb, stanovení fyzického bezpečnostního perimetru
Zničení nebo poškození zařízení v důsledku změn prostředí (změny vlhkosti, teploty ale i přírodní katastrofy)		**Řízení kontinuity činností**	§15(e)	§4 **Řízení aktiv**, **Řízení rizik** §5	havarijní plány
H7	použití neautorizovaného HW (vyměnitelné technické nosiče ve vlastnictví 3. osoby), nedostatky ve formální politice pro používání mobilních zařízení	**Ochrana před škodlivým kódem**	§21(1)(b)	**Řízení aktiv** §4(1)(i)**, Řízení přístupu** §12	monitoring používání výměnných zařízení a datových nosičů
Zneužití vyměnitelných technických nosičů dat		**Řízení přístupu**	§12(2)(e)	**Řízení aktiv** §4(1)(i)	stanovení bezpečnostních opatření pro používání mobilních zařízení a jiných technických zařízení, která povinná osoba nemá ve své správě
	vyřazení nebo opětovné použití záznamových médií bez důkladného vymazání	**Řízení aktiv**	§4(1)(j)	**Řízení aktiv** §4 odst. 1, písm. a) až g)	určení způsobu likvidace technických nosičů dat s ohledem na úroveň aktiv
	nedostatečné kontroly zařízení mimo lokalitu	Řízení aktiv	§4(1)(i)	**Řízení aktiv** §4 odst. 1, písm. a) až g)	stanovení přípustných způsobů používání aktiva
	nedostatečné školení uživatelů a kontrola dodržování ze strany managementu	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)(f)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní; zajištění kontroly dodržování bezpečnostní politiky ze strany uživatelů
		Bezpečnost lidských zdrojů	§9(1)(i)	**Bezpečnost lidských zdrojů** - §9, odst. 1, písm. c), e)	pravidla a postupy pro řešení případů bezpečnostních pravidel uživateli
H8	použití aplikačních programů na špatná data z hlediska času	**Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů**	§22(2)(e)	**Systém řízení bezpečnosti informací** §3	zajištění synchronizace jednotného času technických aktiv nejméně jednou za 24h
poškození dat použitím aplikačních programů na špatná data z hlediska času					

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H9	užití programových prostředků schopných překonat systémové nebo aplikační kontroly	**Aplikační bezpečnost**	§25(2)(a)	**Řízení provozu a komunikací** §10	ochrana aplikací, informací a transakcí před neoprávněnou činností
provedení neoprávněných činností, tj. provedení činností k nimž uživatel nemá oprávnění		Průmyslové, řídící a obdobné systémy	§28(d)	**Řízení aktiv** §4, **Řízení rizik** §5	omezení vzdáleného přístupu k těmto systémům
		Bezpečnost komunikačních sítí	§18(a)(b)(d)(e)	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(l)	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
	nedostatečné školení uživatelů a kontrola dodržování ze strany managementu	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)(f)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní; zajištění kontroly dodržování bezpečnostní politiky ze strany uživatelů
		Bezpečnost lidských zdrojů	§9(1)(i)	**Bezpečnost lidských zdrojů** - §9, odst. 1, písm. c), e)	pravidla a postupy pro řešení případů bezpečnostních pravidel uživateli
	nedostatečné postupy při identifikaci uživatele	**Správa a ověřování identit**	§19	**Řízení přístupu** §12, **Řízení aktiv** §4	nasazení nástroje pro správu a ověření identity uživatelů, autentizační mechanismus
	nedostatečné monitorování činnosti uživatelů a administrátorů, neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	**Bezpečnost lidských zdrojů**	§9(1)(i)	**Bezpečnost lidských zdrojů** §9(1)(c)(e)(h)(f)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
		Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	§22	**Zvládání kybernetických bezpečnostní incidentů** §14, **Řízení aktiv** §4	zaznamenávání bezpečnostních a potřebných provozních událostí důležitých aktiv
	nedostatečné nastavení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	**Organizační bezpečnost**	§6(i)	**Systém řízení bezpečnosti informací** §3	stanovení pravidel pro určení administrátorů
		Řízení přístupových oprávnění	§20(b)	**Řízení aktiv** §4	použití centralizovaného nástroje pro řízení přístupových oprávnění k akivům
		Řízení provozu a komunikací	§10(1)(a)	**Řízení aktiv** §4	stanovení práv a povinností administrátorů, uživatelů a osob zastávajících bezpečnostní role
H10	nedostatečné nastavení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	Organizační bezpečnost	§6(i)	**Systém řízení bezpečnosti informací** §3	stanovení pravidel pro určení administrátorů
zneužití oprávnění ze strany uživatelů a administrátorů, tj. provedení činností k nimž uživateli bylo uděleno oprávnění k jinému než zamýšlenému účelu		Řízení přístupových oprávnění	§20(b)	**Řízení aktiv** §4	použití centralizovaného nástroje pro řízení přístupových oprávnění k aktivům
		Řízení provozu a komunikací	§10(1)(a)	**Řízení aktiv** §4	stanovení práv a povinností administrátorů, uživatelů a osob zastávajících bezpečnostní role
	neodebrání přístupových oprávnění při skončení zaměstnání / změně pozice	**Řízení přístupu**	§12(1)(m)(l)		odebrání nebo změna přístupových oprávnění při ukončení nebo změně smluvního vztahu nebo pozice
	nedostatečné školení uživatelů a kontrola dodržování ze strany managementu	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)(f)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení uživatelů, administrátorů , osob zastávajících bezpečností role a dodavatelů o jejich povinnostech, pravidelné školení, kontrola dodržování, hodnocení účinnosti
		Bezpečnost lidských zdrojů	§9(1)(i)	**Bezpečnost lidských zdrojů** §9(1)(c)(e)(h)(f)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
H11	nedostatečně bezpečná síťová infastruktura, nechráněné komunikační linky	**Bezpečnost komunikačních sítí**	§18	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(l)	segmentace stě, řízení komunikace v rámci sítě, kryptografie, blokace nežádoucí komunikace, využití nástroje pro ochranu integrity komunikační sítě
vzdálená špionáž	přenos odkrytých hesel, použití nedostatečně odolných hesel	**Správa a ověřování identit**	§19	**Řízení přístupu** §12(1)(2)(b)**,** **Kryptografické prostředky** §26	zajištění odolnosti uložených a přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití; vynucování minimálních standardů pro tvorbu hesla
	nechráněný citlivý provoz přenosu	**Kryptografické prostředky**	§26	**Řízení aktiv** §4(1)(i), S**ystém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(l), **Bezpečnost komunikačních sítí** §18	použití aktuálně odolných kryptografických algoritmů a klíčů

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H12	nedostatečně bezpečná síťová infastruktura, nechráněné komunikační linky	**Bezpečnost komunikačních sítí**	§18	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(l)	segmentace sítě, řízení komunikace v rámci sítě, kryptografie, blokace nežádoucí komunikace, využití nástroje pro ochranu integrity komunikační sítě
odposlech	nechráněné připojení do veřejné sítě	**Kryptografické prostředky**	§26	**Řízení aktiv** §4(1)(i), **Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(l), **Bezpečnost komunikačních sítí** §18	použití aktuálně odolných kryptografických algoritmů a klíčů
		Bezpečnost komunikačních sítí	§18	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(l)	segmentace sítě, řízení komunikace v rámci sítě, kryptografie, blokace nežádoucí komunikace, využití nástroje pro ochranu integrity komunikační sítě
H13	nedostatečné školení uživatelů a kontrola dodržování ze strany managementu	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)(f)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení uživatelů, administrátorů , osob zastávajících bezpečností role a dodavatelů o jejich povinnostech, pravidelné školení, kontrola dodržování, hodnocení účinnosti
		Bezpečnost lidských zdrojů	§9(1)(i)	**Bezpečnost lidských zdrojů** §9(1)(c)(e)(h)(f)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	nekontrolované stahování a užívání programů, nedostatečné postupy pro instalaci software do operačních systémů	Řízení aktiv	§4(1)(i)	**Řízení aktiv** §4 odst. 1, písm. a) až g), **Organizační bezpečnost** §6(3)(c) - stanovení garanta aktiva	stanovení přípusných způsobů používání aktiva a pravidla manipulace s aktivy s ohledem na úroveň aktiv
		Řízení přístupu	§12(2)(g)	**Aplikační bezpenost** §25(2), **Správa a ověřování identit** §19, **Řízení přístupových oprávnění** §20	omezení a kontrola používání programových prostředků schopných překonat systémové nebo aplikační kontroly
		Bezpečnost komunikačních sítí	§18(d)	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(j)(e)	aktivní blokace nežádoucí komunikace
	nechráněné připojení do veřejné sítě	**Bezpečnost komunikačních sítí**	§18	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(l)	segmentace sítě, řízení komunikace v rámci sítě, kryptografie, blokace nežádoucí komunikace, využití nástroje pro ochranu integrity komunikační sítě
	použití nedostatečně odolných hesel	**Správa a ověřování identit**	§19	**Řízení přístupu** §12(1)(2)(b)	zajištění odolnosti uložených a přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití, vynucování minimálních standardů pro tvorbu hesla
H14	nechráněné připojení do veřejné sítě	**Bezpečnost komunikačních sítí**	§18	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(l)	segmentace sítě, řízení komunikace v rámci sítě, kryptografie, blokace nežádoucí komunikace, využití nástroje pro ochranu integrity komunikační sítě
instalace zákeřného kódu		**Zvládní kybernetických událostí**	§14(1)	**Zaznamenávání událostí informačního systému** §22-24	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
		Ochrana před škodlivým kódem	§21(1)(a)(e)	**Řízení provozu a komunikací** §10	použití nástroje pro nepřetržitou automatizovanou ochranu před škodlivým kódem a jeho pravidelná aktualizace - nasazováno s ohledem na důležitost aktiv
		Řízení provozu a komunikací	§10(l)(d)	**Řízení aktiv** §4, **Řízení rizik** §5	pravidla a postupy pro zajištění bezpečností síťových služeb, pravidla a postupy pro ochranu před škodlivým kódem
	nedostatečné školení uživatelů a kontrola dodržování ze strany managementu	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)(f)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení uživatelů, administrátorů, osob zastávajících bezpečností role a dodavatelů o jejich povinnostech, pravidelné školení, kontrola dodržování, hodnocení účinnosti
		Bezpečnost lidských zdrojů	§9(1)(i)	**Bezpečnost lidských zdrojů** §9(1)(c)(e)(h)(f)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
	veřejná publikace zdrojového kódu software	Akvizice, vývoj a údržba	§13	**Systém řízení bezpečnosti informací** §3(b), Řízení aktiv §4(1)(h), **Řízení rizik** §5, **Řízení změn** §11	stavenovení požadavků na technické aktivum v projektu akvizice, vývoje a údržby
		Řízení změn	§11	**Systém řízení bezpečnosti informací** §3	analýza rizik, přijetí opatření za účelem snížení nepříznivých dopadů změny
	nekontrolované stahování a užívání programů, používání programů obsahujících známé chyby	Řízení aktiv	§4(1)(i)	**Řízení aktiv** §4 odst. 1, písm. a) až g), **Organizační bezpečnost** §6(3)(c) - stanovení garanta aktiva	stanovení přípusných způsobů používání aktiva a pravidel manipulace s aktivy s ohledem na úroveň aktiv
		Řízení přístupu	§12(2)(g)	**Aplikační bezpenost** §25(2), **Správa a ověřování identit** §19, **Řízení přístupových oprávnění** §20	omezení a kontrola používání programových prostředků schopných překonat systémové nebo aplikační kontroly
		Bezpečnost komunikačních sítí	§18(d)	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(j)(e)	aktivní blokace nežádoucí komunikace

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H15	neexistence potřebné smlouvy (licenční, nájemní, kupní), nedostatečná oprávnění druhé smluvní strany (poskytovatele licence, prodávajícího, pronajímatele), nevhodná formulace smluvních ustanovení	**Řízení dodavatelů**	§8(1)(a),(f)	**Organizační bezpečnost -** §6 odst. 1, písm. c), k), §6(3)(c)	příloha 7, písm. b) - oprávnění užívat data, c) - autorství programového kódu; požadevek dle písm. f) omezen na významné dodavatele
neoprávněné užití technického aktiva, tj. použití bez licence, použití nad rámec licence, použití bez oprávnění	nedostatečné postupy pro zajištění souladu se zákony na ochranu duševního vlastnictví	**Organizační bezpečnost**	§6(1)(b)	**Systém řízení bezpečnosti informací** §3	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu akvizice předmětů chráněných duševním vlastnictvím
	nedostatky ve formálním procesu pro autorizaci veřejně přístupných informací (>> data pocházejí z nedůvěryhodných zdrojů)	**Organizační bezpečnost**	§6(1)(b)	**Systém řízení bezpečnosti informací** §3	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu využití veřejně dostupných dat
H16	nedostatečné postupy při identifikování a odhalení bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů	Řízení provozu a komunikací	§10(1)(c)	**Řízení rizik** §5	postupy pro sledování kybernetických bezpečnostních událostí
		Zvládání kybernetických událostí	§14(1)	**Zaznamenávání událostí informačního systému** §22-24	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
		Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	§22	**Řízení aktiv** §4	zaznamenávání bezpečnostních a potřebných provozních událostí důležitých aktiv
dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	nedostatečná nebo neúplná smlouva o úrovni služeb, porušení smlouvy o úrovni služeb	**Řízení dodavatelů**	§8(1)(a),(d) - všichni, §8(2)(a),(b), příl. 7 písm. k) - významní	**Řízení kontinuity činností** §15(c)	stanovení pravidel pro dodavatele a jejich pravidelné přezkoumávání, u významných též dle přílohy 7 písm. k) - specifikace podmínek pro řízení kontinuity činností
		Řízení provozu a komunikací	§10(1)(a)(f)	**Bezpečnost lidských zdrojů** §9(1)(a)(c)(e)	spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory
	selhání v důsledku přetížení sítě (odolnost směřování)	**Bezpečnost komunikačních sítí**	§18(a)(b)(d)(e)	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(j)(e)	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
		Zvládání kybernetických událostí	§14(1)	**Zaznamenávání událostí informačního systému** §22-24	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
		Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	§22	**Řízení aktiv** §4	zaznamenávání bezpečnostních a potřebných provozních událostí důležitých aktiv
		Průmyslové, řídící a obdobné systémy	§28(c)(e)(f)	**Řízení aktiv** §4, **Řízení rizik** §5	ochrana technických aktiv před využitím známých zranitelností a obnova chodu po kybernetickém bezpečnostním incidentu, vyčlenění od ostatní infastruktury - omezeno na průmyslové, řídící a obdobné specifické systémy
		Zajišťování úrovně dostupnosti informací	§27	§15(c) **Řízení kontinuity činností**, §4 **Řízení aktiv**, **Řízení rizik** §5, **Organizační bezpečnost** §6(3)	zajištění dostupnosti a redundance technických aktiv nezbytných pro provoz informačního a komunikačního systému a to s ohledem na hodnocení podpůrných aktiv
	nedostatky v plánech kontinuity	**Řízení kontinuity činností**	§15	**Systém řízení bezpečnosti informací** §3	plány kontinuity činností
	celkové selhání služby	**Zajišťování úrovně dostupnosti informací**	§27	**Řízení provozu a komunikací** §10, **Řízení kontinuity činností** §15	zajištění redundancie aktiv nezbytných pro zajištění dostupnosti informačního a komunikačního systému; předpokladem je stanovení dostatečné doby pro obnovení chodu

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H17	nedostatečná nebo neúplná smlouva o úrovni služeb, porušení smlouvy o úrovni služeb	**Řízení dodavatelů**	§8(1)(a),(d) - všichni, §8(2)(a),(b), příl. 7 písm. k) - významní	**Řízení kontinuity činností** §15(c)	stanovení pravidel pro dodavatele a jejich pravidelné přezkoumávání, u významných též dle přílohy 7 písm. k) - specifikace podmínek pro řízení kontinuity činností
přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie		**Řízení provozu a komunikací**	§10(1)(a)(f)	**Bezpečnost lidských zdrojů** §9(1)(a)(c)(e)	spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory
	selhání v důsledku přetížení sítě (odolnost směřování)	**Bezpečnost komunikačních sítí**	§18(a)(b)(d)(e)	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(j)(e)	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
		Zvládání kybernetických událostí	§14(1)	**Zaznamenávání událostí informačního systému** §22-24	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
		Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	§22	**Řízení aktiv** §4	zaznamenávání bezpečnostních a potřebných provozních událostí důležitých aktiv
		Průmyslové, řídící a obdobné systémy	§28(c)(e)(f)	**Řízení aktiv** §4, **Řízení rizik** §5	ochrana technických aktiv před využitím známých zranitelností a obnova chodu po kybernetickém bezpečnostním incidentu, vyčlenění od ostatní infastruktury - omezeno na průmyslové, řídící a obdobné specifické systémy
		Řízení kontinuity činností	§15	§4 **Řízení aktiv**, **Řízení rizik** §5, **Organizační bezpečnost** §6(3)	stanovení politiky a plánu kontinuity činností a provádí opatření ke zvýšení odolnosti systému
	nedostatečné postupy při identifikování a odhalení bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů	Řízení provozu a komunikací	§10(1)(c)	**Řízení rizik** §5	postupy pro sledování kybernetických bezpečnostních událostí
		Zvládání kybernetických událostí	§14(1)	**Zaznamenávání událostí informačního systému** §22-24	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
		Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	§22	**Řízení aktiv** §4	zaznamenávání bezpečnostních a potřebných provozních událostí důležitých aktiv
H18	nedostatečné bezpečnostní školení	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)(f)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Systém řízení bezpečnosti informací** §3	poučení uživatelů, administrátorů , osob zastávajících bezpečností role a dodavatelů o jejich povinnostech, pravidelné školení, kontrola dodržování, hodnocení účinnosti
porušení bezpečnostní politiky		**Bezpečnost lidských zdrojů**	§9(1)(i)	§9(1)(c)(e)(h)(f), **Systém řízení bezpečnosti informací** §3	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
		Zvládání kybernetických událostí	§14(1)	**Zaznamenávání událostí informačního systému** §22-24	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
	nedostatečné provádění pravidelných auditů / dohledu	Audit kybernetické bezpečnosti	§16	**Systém řízení bezpečnosti informací** §3	pravidelný audit kybernetické bezpečnosti
H19	nedostatky v postupech pro identifikaci a posouzení rizik	**Systém řízení bezpečnosti informací**	§3	N/A	určení organizačních částí a aktiv, kterých se systém řízení bezpečnosti týká
chybná identifikace technických aktiv					

Personální aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H20	neschopnost ověřit kvalifikaci subdodavatele v rámci výběrového řízení	Řízení dodavatelů	§8(2)	**Řízení rizik** §5	hodnocení rizik v rámci výběrového řízení a před uzavřením smlouvy - omezeno na významné dodavatele
nedodržení smluvního závazku ze strany subdodavatele		**Organizační bezpečnost**	§6(1)(b)	**Systém řízení bezpečnosti** §3	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu výběru subdodavatelů
	nejednoznačná / nedostatečná definice závazku subdodavatele	**Řízení dodavatelů**	§8(1)(a)(d)(f)(2)(b)	**Systém řízení bezpečnosti** §3	stanovení pravidel pro dodavatele, seznámení dodavatele s pravidly, u významných stanovení způsobů a úrovní realizace bezpečnostních oprávnění a rozsah vzájemné smluvní odpovědnosti
	neschopnost včasného odhalení pochybení ze strany subdodavatelů	**Řízení dodavatelů**	§8(1)(g)(2)(c)	**Systém řízení bezpečnosti** §3, **Řízení rizik** §5	pravidelné přezkoumávání smluv s významnými dodavateli, hodnocení rizik a pravidelná kontrola zavedených bezpečnostních opatření - omezeno na významné dodavatele
		Bezpečnost lidských zdrojů	§9(1)(c)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení dodavatelů o jejich povinnostech, pravidelné školení, kontrola dodržování, hodnocení účinnosti
		Bezpečnost lidských zdrojů	§9(1)(i)	§9(1)(c)(e)(h)(f)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
H21	nedostatečné poučení / vzdělávání zaměstnanců	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)(f)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení uživatelů, administrátorů , osob zastávajících bezpečností role a dodavatelů o jejich povinnostech, pravidelné školení
pochybení ze strany zaměstnanců (včetně trestné činnosti)	nejednoznačná / nedostatečná definice povinností zaměstnance	Organizační bezpečnost	§6(1)(b)	**Systém řízení bezpečnosti informací** §3	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu stanovení pracovních nápní zaměstnanců
	neschopnost včasného odhalení pochybení ze strany zaměstnanců	**Bezpečnost lidských zdrojů**	§9(1)(f)(h)	§9(1)(c)(e) - **Bezpečnost lidských zdrojů**	kontrola dodržování bezpečnostní politiky ze strany uživatelů, administrátorů, osob zastávající bezpečnostní role, hodnocení účinnosti plánu rozvoje bezpečnostního povědomí
		Bezpečnost lidských zdrojů	§9(1)(i)	§9(1)(c)(e)(h)(f)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
	neschopnost identifikace problematických vzorců chováním v rámci výběrového řízení	Organizační bezpečnost	§6(1)(b)	**Systém řízení bezpečnosti informací** §3	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu výběru zaměstnanců

Personální aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H22	nedostatečné vzdělávání zaměstnanců	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b)	poučení uživatelů, administrátorů , osob zastávajících bezpečností role a dodavatelů o jejich povinnostech, pravidelné školení
nedostatečná odborná úroveň	neschopnost ověřit kvalifikaci uchazeče v rámci výběrového řízení	Bezpečnostní role	§7	§6 **Organizační bezpečnost** - odst. 3 až 6 - povinnost ustanovit bezpečnostní role	úroveň vzdělání stanovena pouze pro vymezené bezpečnostní Rrole
	nedostatečná míra nezávislé kontroly s cílem včas identifikovat chybějící odbornost	**Bezpečnost lidských zdrojů**	§9(1)(i)	§9(1)(c)(e)(h)(f)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
H23	absence konkureční doložky ve smlouvě	**Organizační bezpečnost**	§6(1)(b)	**Systém řízení bezpečnosti informací** §3, **Řízení rizik** §5	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu vyjednávání a uzavírání pracovních smluv
přechod klíčového personálního aktiva ke konkurenci					
H24	absence ujednání o zachovávání mlčenlivosti i po odchodu / zákonného povinnosti mlčenlivosti	**Organizační bezpečnost**	§6(1)(j)	**Systém řízení bezpečnosti informací** §3, **Řízení rizik** §5	zajištění, aby byla zachovávána mlčenlivost administrátorů a osob zastávajících bezpečnostní role - vztahuje se pouze na vybrané skupiny
vyzrazení informací		Řízení provozu a komunikací	§10(1)(i)	**Systém řízení bezpečnosti informací** §3, **Řízení rizik** §5	pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu
	nedostatečné poučení příjemců	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b)	poučení uživatelů, administrátorů , osob zastávajících bezpečností role a dodavatelů o jejich povinnostech, pravidelné školení
		Bezpečnost lidských zdrojů	§9(1)(i)	§9(1)(c)(e)(h)(f)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
H25	neexistující / nedostatečná exit procedura	**Bezpečnost lidských zdrojů**	§9(1)(g)	**Systém řízení bezpečnosti informací** §3, **Řízení rizik** §5	zajištění, aby v případě ukončení sml. vztahu s administrátory a osobami zastávajícími bezp. role byla předána odpovědnost - omezeno na vybrané skupiny
nedostatečné předání agendy / ztráta know-how při odchodu zaměstnance /		**Organizační bezpečnost**	§6(1)(b)	**Systém řízení bezpečnosti informací** §3, **Řízení rizik** §5	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu odchodu zaměstnance / dodavatele
H26	nedostatky v postupech pro identifikaci a posouzení rizik	**Systém řízení bezpečnosti informací**	§3	N/A	určení organizačních částí a aktiv, kterých se systém řízení bezpečnosti týká
chybná identifikace personálních aktiv					

SEZNAM POUŽITÝCH ZDROJŮ:

[1] *Metodika k vodítkům pro hodnocení dopadů* [online]. Národní úřad pro kybernetickou a informační bezpečnost. 1.2. Česká republika, 2018 [cit. 2019-12-30]. Dostupné z https://www.govcert.cz/download/kii-vis/Metodika_k_voditkum_pro_hodnoceni_dopadu_NUKIB_v.1.2_s_prilohou.pdf

[2] *Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)* . In: *Sbírka zákonů* . 28.5.2018. ISSN 1211-1244