

rizika = hrozby x zranitelnosti x primární informační aktiva

Analýza rizik - státní správa

Id hrozby Id zranitelnosti Hodnota zranitelnosti / hrozby			Četnost rizik Název hrozby/zranitelnosti Hodnota dopadu aktiva:		součin hodnota hrozby a zranitelnosti		Registru primárních aktiv														Pomocné součty											
							Důvěrnost PIA				Integrita PIA		Dostupnost PIA		Maximum hodnoty rizika pro související primární aktiva																	
							A1.1	A1.1.1	A1.1.2	A1.1.3	A1.1.4	A1.2	A1.2.1	A1.2.2	A1.3	A1.3.1	A1.3.2	A1.3.3	A1													
							A - Utažované informace a zvláštní skutečnosti	B - Osobní údaje			C - Informace interní důvěrné	D - Ostatní informace	I1 - zálohování databází nebo DDDÚ		I2 - zálohování na běžný fileserver		D1 - 1 den		D1 - 2-3 dny		D1 - nad 3 dny		Maximum hodnoty rizika pro související primární aktiva									
							3	2	2	1	0	3	2	0	0	3	2	1	0	0												
Z1.1	2	Nedostatečná ochrana vnějšího perimetru				0	0	0	0	0	0	0	0	0	0	0	0	x	x	0												
H1.1	x	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a admin.				0														0												
H1.2	x	Poškození nebo selhání hardwaru nebo softwaru.				0														0												
H1.3	x	Zneužití identity jiné fyzické osoby.				0														0												
H1.4	x	Užívání softwaru v rozporu s licenčními podmínkami.				0														0												
H1.5	x	Kybernetický útok z vnější komunikační sítě.				0														0												
H1.6	x	Škodlivý kód např. viry, spyware, trojské koně apod.				0														0												
H1.7	x	Nedostatky při plnění služeb informačního systému.				0														0												
H1.8	1	Projevy přírodních jevů např. povodně, klimatické jevy apod.				2	6	4	4	2		6	4				6			6												
H1.9	x	Přerušení dodávky komunikačních služeb nebo elektrické energie.				0														0												
H1.10	x	Zneužití nebo neoprávněná modifikace údajů.				0														0												
H1.11	3	Trvale působící pokročilé hrozby (APT - Advanced Persistent Threat)				6	18	12	12	6		18	12				18			18												
H1.12	2	Odcizení nebo poškození fyzického zařízení (aktiva).				4	12	8	8	4		12	8				12			12												
Z1.2	3	Nedostatečné povědomí uživatelů a administrátorů				x	0	0	0	0	0	0	0	0	0	0	0	0	0	0												
H1.1	2	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a admin.				6		12	12	6		18	12				18	12	6	18												
H1.2	2	Poškození nebo selhání hardwaru nebo softwaru.				6		12	12	6		18	12				18	12	6	18												
H1.3	x	Zneužití identity jiné fyzické osoby.				0														0												
H1.4	x	Užívání softwaru v rozporu s licenčními podmínkami.				0														0												
H1.5	x	Kybernetický útok z vnější komunikační sítě.				0														0												
H1.6	3	Škodlivý kód např. viry, spyware, trojské koně apod.				9		18	18	9		27	18				27	18	9	27												
H1.7	x	Nedostatky při plnění služeb informačního systému.				0														0												
H1.8	x	Projevy přírodních jevů např. povodně, klimatické jevy apod.				0														0												
																					Z1.1		Nízká: 11		Střední: 16		Vysoká: 0		Kritická: 0		Celkem: 27	
																					Z1.2		Nízká: 10		Střední: 36		Vysoká: 4		Kritická: 0		Celkem: 50	

H1.9	x	Přerušení dodávky komunikačních služeb nebo elektrické energie.	0													0
H1.10	x	Zneužití nebo neoprávněná modifikace údajů.	0													0
H1.11	3	Trvale působící pokročilé hrozby (APT - Advanced Persistent Threat)	9	18	18	9		27	18		27	18	9		27	
H1.12	2	Odcizení nebo poškození fyzického zařízení (aktiva).	6	12	12	6		18	12		18	12	6		18	
Z1.3	3	Nedostatečná údržba zařízení		0	0	0	0	0	0	0	0	x	x			
H1.1	x	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a admin.	0													0
H1.2	2	Poškození nebo selhání hardwaru nebo softwaru.	6	18	12	12	6		18	12		18				18
H1.3	x	Zneužití identity jiné fyzické osoby.	0													0
H1.4	x	Užívání softwaru v rozporu s licenčními podmínkami.	0													0
H1.5	x	Kybernetický útok z vnější komunikační sítě.	0													0
H1.6	x	Škodlivý kód např. viry, spyware, trojské koně apod.	0													0
H1.7	x	Nedostatky při plnění služeb informačního systému.	0													0
H1.8	x	Projevy přírodních jevů např. povodně, klimatické jevy apod.	0													0
H1.9	x	Přerušení dodávky komunikačních služeb nebo elektrické energie.	0													0
H1.10	x	Zneužití nebo neoprávněná modifikace údajů.	0													0
H1.11	3	Trvale působící pokročilé hrozby (APT - Advanced Persistent Threat)	9	27	18	18	9		27	18		27				27
H1.12	x	Odcizení nebo poškození fyzického zařízení (aktiva).	0													0
Z1.4	3	Nevhodné nastavení přístupových oprávnění		0	0	0	0	0	0	0	0	0	0	x		
H1.1	2	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a admin.	6	18	12	12	6		18	12		18	12			18
H1.2	x	Poškození nebo selhání hardwaru nebo softwaru.	0													0
H1.3	2	Zneužití identity jiné fyzické osoby.	6	18	12	12	6		18	12		18	12			18
H1.4	x	Užívání softwaru v rozporu s licenčními podmínkami.	0													0
H1.5	3	Kybernetický útok z vnější komunikační sítě.	9	27	18	18	9		27	18		27	18			27
H1.6	3	Škodlivý kód např. viry, spyware, trojské koně apod.	9	27	18	18	9		27	18		27	18			27
H1.7	x	Nedostatky při plnění služeb informačního systému.	0													0
H1.8	x	Projevy přírodních jevů např. povodně, klimatické jevy apod.	0													0
H1.9	x	Přerušení dodávky komunikačních služeb nebo elektrické energie.	0													0
H1.10	x	Zneužití nebo neoprávněná modifikace údajů.	0													0
H1.11	3	Trvale působící pokročilé hrozby (APT - Advanced Persistent Threat)	9	27	18	18	9		27	18		27	18			27
H1.12	x	Odcizení nebo poškození fyzického zařízení (aktiva).	0													0
Z1.5	3	Nedostatečné schopnosti při identifikování a odhalení negativních bezpečnostních jevů, událostí a incidentů		0	0	0	0	0	0	0	0	0	0	0		

Z1.3

Nízká: 4
Střední: 11
Vysoká: 3
Kritická: 0
Celkem: 18

Z1.4

Nízká: 10
Střední: 31
Vysoká: 9
Kritická: 0
Celkem: 50

Z1.3

Nízká: 4

Střední: 11

Vysoká: 3

Kritická: 0

Celkem: 18

Z1.4

Nízká: 10

Střední: 31

Vysoká: 9

Kritická: 0

Celkem: 50

H1.1	2	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a admin.	6	18	12	12	6	18	12	18	12	6	18	Z1.5
H1.2	2	Poškození nebo selhání hardwaru nebo softwaru.	6	18	12	12	6	18	12	18	12	6	18	Nízká: 28
H1.3	2	Zneužití identity jiné fyzické osoby.	6	18	12	12	6	18	12	18	12	6	18	Střední: 95
H1.4	1	Užívání softwaru v rozporu s licenčními podmínkami.	3	9	6	6	3	9	6	9	6	3	9	Vysoká: 9
H1.5	3	Kybernetický útok z vnější komunikační sítě.	9	27	18	18	9	27	18	27	18	9	27	Kritická: 0
H1.6	3	Škodlivý kód např. viry, spyware, trojské koně apod.	9	27	18	18	9	27	18	27	18	9	27	Celkem: 132
H1.7	2	Nedostatky při plnění služeb informačního systému.	6	18	12	12	6	18	12	18	12	6	18	
H1.8	1	Projevy přírodních jevů např. povodně, klimatické jevy apod.	3	9	6	6	3	9	6	9	6	3	9	
H1.9	2	Přerušení dodávky komunikačních služeb nebo elektrické energie.	6	18	12	12	6	18	12	18	12	6	18	
H1.10	2	Zneužití nebo neoprávněná modifikace údajů.	6	18	12	12	6	18	12	18	12	6	18	
H1.11	3	Trvale působící pokročilé hrozby (APT - Advanced Persistent Threat)	9	27	18	18	9	27	18	27	18	9	27	
H1.12	2	Odcizení nebo poškození fyzického zařízení (aktiva).	6	18	12	12	6	18	12	18	12	6	18	
Z1.6	2	Nedostatečné monitorování činnosti koncových uživatelů, neschopnost odhalit nevhodné či závažné způsoby chování		0	0	0	0	0	0	0	0	0	0	
H1.1	2	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a admin.	4	12	8	8	4	12	8	12	8	4	12	Z1.6
H1.2	2	Poškození nebo selhání hardwaru nebo softwaru.	4	12	8	8	4	12	8	12	8	4	12	Nízká: 28
H1.3	2	Zneužití identity jiné fyzické osoby.	4	12	8	8	4	12	8	12	8	4	12	Střední: 49
H1.4	1	Užívání softwaru v rozporu s licenčními podmínkami.	2	6	4	4	2	6	4	6	4	2	6	Vysoká: 0
H1.5	x	Kybernetický útok z vnější komunikační sítě.	0										0	Kritická: 0
H1.6	3	Škodlivý kód např. viry, spyware, trojské koně apod.	6	18	12	12	6	18	12	18	12	6	18	Celkem: 77
H1.7	x	Nedostatky při plnění služeb informačního systému.	0										0	
H1.8	x	Projevy přírodních jevů např. povodně, klimatické jevy apod.	0										0	
H1.9	x	Přerušení dodávky komunikačních služeb nebo elektrické energie.	0										0	
H1.10	2	Zneužití nebo neoprávněná modifikace údajů.	4	12	8	8	4	12	8	12	8	4	12	
H1.11	3	Trvale působící pokročilé hrozby (APT - Advanced Persistent Threat)	6	18	12	12	6	18	12	18	12	6	18	
H1.12	x	Odcizení nebo poškození fyzického zařízení (aktiva).	0										0	
Z1.7	2	Nedostatečné stanovení bezpečnostních pravidel, nepřesné či nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezp. rolí		0	0	0	0	0	0	0	0	0	0	
H1.1	2	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a admin.	4	12	8	8	4	12	8	12	8	4	12	Z1.7
H1.2	2	Poškození nebo selhání hardwaru nebo softwaru.	4	12	8	8	4	12	8	12	8	4	12	Nízká: 38
H1.3	2	Zneužití identity jiné fyzické osoby.	4	12	8	8	4	12	8	12	8	4	12	Střední: 72
H1.4	1	Užívání softwaru v rozporu s licenčními podmínkami.	2	6	4	4	2	6	4	6	4	2	6	Vysoká: 0
H1.5	3	Kybernetický útok z vnější komunikační sítě.	6	18	12	12	6	18	12	18	12	6	18	Kritická: 0
H1.6	3	Škodlivý kód např. viry, spyware, trojské koně apod.	6	18	12	12	6	18	12	18	12	6	18	Celkem: 110

H1.7	x	Nedostatků při plnění služeb informačního systému.	0												0	
H1.8	x	Projevy přírodních jevů např. povodně, klimatické jevy apod.	0												0	
H1.9	2	Přerušení dodávky komunikačních služeb nebo elektrické energie.	4	12	8	8	4	12	8	12	8	4	12			
H1.10	2	Zneužití nebo neoprávněná modifikace údajů.	4	12	8	8	4	12	8	12	8	4	12			
H1.11	3	Trvale působící pokročilé hrozby (APT - Advanced Persistent Threat)	6	18	12	12	6	18	12	18	12	6	18			
H1.12	2	Odcizení nebo poškození fyzického zařízení (aktiva).	4	12	8	8	4	12	8	12	8	4	12			
Z2.1	3	Nedostatečná ochrana prostředků infrastruktury		0	0	0	0	0	0	0	0	x	x			
H2.1	3	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany administrátorů	9	27	18	18	9	27	18	27			27		Z2.1	
H2.2	3	Pochybení ze strany zaměstnanců.	9	27	18	18	9	27	18	27			27		Nízká:	12
H2.3	2	Kybernetický útok z vnitřní sítě, zneužití vnitřních prostředků, sabotáž.	6	18	12	12	6	18	12	18			18		Střední:	36
H2.4	2	Dlouhodobé přerušení komunikačních služeb, dodávky elektrické energie nebo jiných důležitých služeb.	6	18	12	12	6	18	12	18			18		Vysoká:	6
H2.5	2	Nedostatek či nedostupnost zaměstnanců s potřebnou odbornou úrovní.	6	18	12	12	6	18	12	18			18		Kritická:	0
H2.6	2	Cílený kybernetický útok pomocí sociálního inženýrství, použití špiónážních technik.	6	18	12	12	6	18	12	18			18		Celkem:	54
H2.7	x	Zneužití vyměnitelných paměťových médií	0											0		
Z2.2	3	Nevhodná bezpečnostní architektura		0	0	0	0	0	0	0	0	0	0			
H2.1	3	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany administrátorů	9	27	18	18	9	27	18	27	18	9	27		Z2.2	
H2.2	3	Pochybení ze strany zaměstnanců.	9	27	18	18	9	27	18	27	18	9	27		Nízká:	10
H2.3	2	Kybernetický útok z vnitřní sítě, zneužití vnitřních prostředků, sabotáž.	6	18	12	12	6	18	12	18	12	6	18		Střední:	39
H2.4	2	Dlouhodobé přerušení komunikačních služeb, dodávky elektrické energie nebo jiných důležitých služeb.	6	18	12	12	6	18	12	18	12	6	18		Vysoká:	6
H2.5	x	Nedostatek či nedostupnost zaměstnanců s potřebnou odbornou úrovní.	0											0	Kritická:	0
H2.6	2	Cílený kybernetický útok pomocí sociálního inženýrství, použití špiónážních technik.	6	18	12	12	6	18	12	18	12	6	18		Celkem:	55
H2.7	x	Zneužití vyměnitelných paměťových médií	0											0		
Z2.3	1	Nedostatečná míra nezávislé kontroly		0	0	0	0	0	0	0	0	0	0			
H2.1	3	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany administrátorů	3	9	6	6	3	9	6	9	6	3	9		Z2.3	
H2.2	3	Pochybení ze strany zaměstnanců.	3	9	6	6	3	9	6	9	6	3	9		Nízká:	28
H2.3	2	Kybernetický útok z vnitřní sítě, zneužití vnitřních prostředků, sabotáž.	2	6	4	4	2	6	4	6	4	2	6		Střední:	16
H2.4	2	Dlouhodobé přerušení komunikačních služeb, dodávky elektrické energie nebo jiných důležitých služeb.	2	6	4	4	2	6	4	6	4	2	6		Vysoká:	0
H2.5	x	Nedostatek či nedostupnost zaměstnanců s potřebnou odbornou úrovní.	0											0	Kritická:	0
H2.6	2	Cílený kybernetický útok pomocí sociálního inženýrství, použití špiónážních technik.	2	6	4	4	2	6	4	6	4	2	6		Celkem:	44

H2.7	x	Zneužití vyměnitelných paměťových médií	0												0
Z2.4	3	Neschopnost odhalit nevhodné nebo závadné způsoby chování		0	0	0	0	0	0	0	0	0	0	0	
H2.1	3	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany administrátorů	9	27	18	18	9	27	18	27	18	9	27		Z2.4
H2.2	3	Pochybení ze strany zaměstnanců.	9	27	18	18	9	27	18	27	18	9	27		Nízká: 12
H2.3	2	Kybernetický útok z vnitřní sítě, zneužití vnitřních prostředků, sabotáž.	6	18	12	12	6	18	12	18	12	6	18		Střední: 48
H2.4	2	Dlouhodobé přerušení komunikačních služeb, dodávky elektrické energie nebo jiných důležitých služeb.	6	18	12	12	6	18	12	18	12	6	18		Vysoká: 6
H2.5	x	Nedostatek či nedostupnost zaměstnanců s potřebnou odbornou úrovní.	0										0		Kritická: 0
H2.6	2	Cílený kybernetický útok pomocí sociálního inženýrství, použití špiónážních technik.	6	18	12	12	6	18	12	18	12	6	18		Celkem: 66
H2.7	x	Zneužití vyměnitelných paměťových médií	0										0		

Četnost rizik:

	234
Nízká:	63
Střední:	447
Vysoká:	43
Kritická:	0
Celkem:	553

Pomocné výpočty četnosti rizik

9	10	10	10	10	10	10	8	7
0	6	6	21	0	6	0	5	19
47	59	59	44	50	59	50	49	30
13	0	0	0	15	0	15	0	0
0	0	0	0	0	0	0	0	0

Kontrolní součty

	0
Nízká:	191
Střední:	449
Vysoká:	43
Kritická:	0
Celkem:	683

Maximum:

27 18 18 9 0 27 18 0 27 18 9

Hodnota rizika je součinem hodnot pravděpodobnosti výskytu hrozby, hodnoty zranitelnosti aktiva vůči relevantní hrozbě a hodnoty dopadu

Stupeň rizika je odvozen od hodnoty rizika dle tabulky níže.

Stupeň rizika	Popis rizika	Interval formát	Interval četnost
Nízká:	Riziko je považováno za zbytkové.	1	4
Střední:	Riziko může být sníženo méně náročnými opatřeními nebo případně vyšší náročnosti opatření akceptováno.	5	18
Vysoká:	Riziko je dlouhodobě nepřijatelné a musí být zahájeny systematické kroky k jeho odstranění.	19	32
Kritická:	Riziko je nepřijatelné a musí být neprodleně zahájeny kroky k jeho odstranění.	33	65

Hodnocení zranitelnosti

Pro hodnocení zranitelnosti je definována lineární procentuální stupnice, která vyjadřuje

Nízká		Zranitelnost neexistuje nebo je málo pravděpodobná	0-25%	1
Střední		Zranitelnost je málo pravděpodobná až pravděpodobná	26-50%	2
Vysoká		Zranitelnost je pravděpodobná až velmi pravděpodobná	51-75%	3
Kritická		Zranitelnost je velmi pravděpodobná až víceméně jisté zneužití	76-100%	4
		Nehodnoceno - hrozba je vůči aktivu irelevantní		x

Automatická akceptace rizik

1. Pouze nízká rizika
2. Nízká a střední rizika