

rizika = hrozby x zranitelnosti x primární informační aktiva

Analýza rizik - soukromá organizace

[illegible]

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

Z1.3

Nízká: 10

Střední: 12

Vysoká: 0

Kritická: 0

Celkem: 22

Z1.4

Nízká: 19

Střední: 58

Vysoká: 0

Kritická: 0

Celkem: 77

Z1.5

Nízká: 22

H1.3	x	Zneužití identity jiné fyzické osoby.	0												0	Střední: 55
H1.4	x	Užívání softwaru v rozporu s licenčními podmínkami.	0												0	Vysoká: 0
H1.5	3	Kybernetický útok z vnější komunikační sítě.	6	18	18	12	6	18	18	6	18	18	6	18	18	Kritická: 0
H1.6	3	Škodlivý kód např. viry, spyware, trojské koně apod.	6	18	18	12	6	18	18	6	18	18	6	18	18	Celkem: 77
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	12	8	4	12	12	4	12	12	4	12	12	
H1.10	2	Zneužití nebo neoprávněná modifikace údajů.	4	12	12	8	4	12	12	4	12	12	4	12	12	
H1.11	2	Trvale působící pokročilé hrozby (APT - Advanced Persistent Threat)	4	12	12	8	4	12	12	4	12	12	4	12	12	
H1.12	x	Odcizení nebo poškození fyzického zařízení (aktiva).	0												0	
Z1.6	2	Nedostatečné monitorování činnosti koncových uživatelů, neschopnost odhalit nevhodné či závadné způsoby chování		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.	4	12	12	8	4	12	12	4	12	12	4	12	12	Z1.6
H1.2	2	Poškození nebo selhání hardwaru nebo softwaru.	4	12	12	8	4	12	12	4	12	12	4	12	12	Nízká: 26
H1.3	3	Zneužití identity jiné fyzické osoby.	6	18	18	12	6	18	18	6	18	18	6	18	18	Střední: 62
H1.4	2	Užívání softwaru v rozporu s licenčními podmínkami.	4	12	12	8	4	12	12	4	12	12	4	12	12	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	18	12	6	18	18	6	18	18	6	18	18	Celkem: 88
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	x	Přerušení dodávky komunikačních služeb nebo elektrické energie.	0												0	
H1.10	2	Zneužití nebo neoprávněná modifikace údajů.	4	12	12	8	4	12	12	4	12	12	4	12	12	
H1.11	2	Trvale působící pokročilé hrozby (APT - Advanced Persistent Threat)	4	12	12	8	4	12	12	4	12	12	4	12	12	
H1.12	2	Odcizení nebo poškození fyzického zařízení (aktiva).	4	12	12	8	4	12	12	4	12	12	4	12	12	
Z1.7	1	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	0		
H1.1	2	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a admin.	2	6	6	4	2	6	6	2	6	6	2	6	6	Z1.7
H1.2	2	Poškození nebo selhání hardwaru nebo softwaru.	2	6	6	4	2	6	6	2	6	6	2	6	6	Nízká: 47
H1.3	3	Zneužití identity jiné fyzické osoby.	3	9	9	6	3	9	9	3	9	9	3	9	9	Střední: 63
H1.4	2	Užívání softwaru v rozporu s licenčními podmínkami.	2	6	6	4	2	6	6	2	6	6	2	6	6	Vysoká: 0
H1.5	3	Kybernetický útok z vnější komunikační sítě.	3	9	9	6	3	9	9	3	9	9	3	9	9	Kritická: 0
H1.6	3	Škodlivý kód např. viry, spyware, trojské koně apod.	3	9	9	6	3	9	9	3	9	9	3	9	9	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.	2	6	6	4	2	6	6	2	6	6	2	6	6	

H1.10	2	Zneužití nebo neoprávněná modifikace údajů.	2	6	6	4	2	6	6	2	6	6	6	2	6
H1.11	2	Trvale působící pokročilé hrozby (APT - Advanced Persistent Threat)	2	6	6	4	2	6	6	2	6	6	6	2	6
H1.12	2	Odcizení nebo poškození fyzického zařízení (aktiva).	2	6	6	4	2	6	6	2	6	6	6	2	6
Z2.1	2	Nedostatečná ochrana prostředků infrastruktury		0	0	0	0	0	0	0	0	0	0	0	
H2.1	2	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany administrátorů	4	12	12	8	4	12	12	4	12	12	12	4	12
H2.2	3	Pochybení ze strany zaměstnanců.	6	18	18	12	6	18	18	6	18	18	18	6	18
H2.3	1	Kybernetický útok z vnitřní sítě, zneužití vnitřních prostředků, sabotáž.	2	6	6	4	2	6	6	2	6	6	6	2	6
H2.4	1	Dlouhodobé přerušení komunikačních služeb, dodávky elektrické energie nebo jiných důležitých služeb.	2	6	6	4	2	6	6	2	6	6	6	2	6
H2.5	2	Nedostatek či nedostupnost zaměstnanců s potřebnou odbornou úrovní.	4	12	12	8	4	12	12	4	12	12	12	4	12
H2.6	2	Cílený kybernetický útok pomocí sociálního inženýrství, použití špiónážních technik.	4	12	12	8	4	12	12	4	12	12	12	4	12
H2.7	x	Zneužití vyměnitelných paměťových médií	0												0
Z2.2	2	Nevhodná bezpečnostní architektura		0	0	0	0	0	0	0	0	0	0	0	
H2.1	2	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany administrátorů	4	12	12	8	4	12	12	4	12	12	12	4	12
H2.2	3	Pochybení ze strany zaměstnanců.	6	18	18	12	6	18	18	6	18	18	18	6	18
H2.3	1	Kybernetický útok z vnitřní sítě, zneužití vnitřních prostředků, sabotáž.	2	6	6	4	2	6	6	2	6	6	6	2	6
H2.4	1	Dlouhodobé přerušení komunikačních služeb, dodávky elektrické energie nebo jiných důležitých služeb.	2	6	6	4	2	6	6	2	6	6	6	2	6
H2.5	2	Nedostatek či nedostupnost zaměstnanců s potřebnou odbornou úrovní.	4	12	12	8	4	12	12	4	12	12	12	4	12
H2.6	2	Cílený kybernetický útok pomocí sociálního inženýrství, použití špiónážních technik.	4	12	12	8	4	12	12	4	12	12	12	4	12
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	0	
H2.1	2	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany administrátorů	2	6	6	4	2	6	6	2	6	6	6	2	6
H2.2	3	Pochybení ze strany zaměstnanců.	3	9	9	6	3	9	9	3	9	9	9	3	9
H2.3	1	Kybernetický útok z vnitřní sítě, zneužití vnitřních prostředků, sabotáž.	1	3	3	2	1	3	3	1	3	3	3	1	3
H2.4	1	Dlouhodobé přerušení komunikačních služeb, dodávky elektrické energie nebo jiných důležitých služeb.	1	3	3	2	1	3	3	1	3	3	3	1	3
H2.5	2	Nedostatek či nedostupnost zaměstnanců s potřebnou odbornou úrovní.	2	6	6	4	2	6	6	2	6	6	6	2	6
H2.6	2	Cílený kybernetický útok pomocí sociálního inženýrství, použití špiónážních technik.	2	6	6	4	2	6	6	2	6	6	6	2	6
H2.7	x	Zneužití vyměnitelných paměťových médií	0												0
Z2.4	2	Neschopnost odhalit nevhodné nebo závadné způsoby chování		0	0	0	0	0	0	0	0	0	0	0	

Z2.1

Nízká: 23

Střední: 43

Vysoká: 0

Kritická: 0

Celkem: 66

Z2.2

Nízká: 23

Střední: 43

Vysoká: 0

Kritická: 0

Celkem: 66

Z2.3

Nízká: 45

Střední: 32

Vysoká: 0

Kritická: 0

Celkem: 77

	177
Nízka:	207
Střední:	463
Vysoká:	0
Kritická:	0
Celkem:	670

10	10	10	10	10		10	10		10	10	10
3	3	24	55	3		3	55		3	3	55
64	64	43	12	64		64	12		64	64	12
0	0	0	0	0		0	0		0	0	0
0	0	0	0	0		0	0		0	0	0

	0
Nízka:	279
Střední:	480
Vysoká:	0
Kritická:	0
Celkem:	759

18	18	12	6	18	0	18	6	0	18	18	6
----	----	----	---	----	---	----	---	---	----	----	---

Stupeň rizika je odvozen od hodnoty rizika dle tabulky níže.

Stupeň rizika je odvozen od hodnoty rizika dle tabulky níže.		Interval	Interval	
Stupeň rizika	Popis rizika	formát	četnost	
Nízká:	Riziko je považováno za zbytkové.	1	4	0
Střední:	Riziko může být sníženo méně náročnými opatřeními nebo případně vyšší náročnosti opatření akceptováno.	5	18	4
Vysoká:	Riziko je dlouhodobě nepřijatelné a musí být zahájeny systematické kroky k jeho odstranění.	19	32	18
Kritická:	Riziko je nepřijatelné a musí být neprodleně zahájeny kroky k jeho odstranění.	33	65	32

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