

Analýza rizik

Pravděpodobnost

- 1 – situace se nikdy nestala a není pravděpodobné, že by se stát měla
- 2 – situace se stala a dá se předpokládat, že nastane znovu
- 3 – situace se může často opakovat

Dopad

- 1 – událost nemá žádný nebo jen velmi malý dopad
- 2 – událost může znamenat ohrožení práv a svobod subjektů údajů nebo dopad na technické prostředky
- 3 – událost má zcela jistě dopad na práva a svobody subjektů údajů nebo významný dopad na technické prostředky

		3	6	9
	2	2	4	6
	1	1	2	1
		1	2	3

Případ č. 1

Zranitelnost	Hrozba	Pravděpodobnost	Dopad	Risk skóre	Riziko	Opatření ke snížení nebo eliminaci rizika
Nedostatečná autentizace	Neoprávněný přístup k datům: Krádež	1	3	3	Mírné	Organizační opatření, heslová politika, šifrování
Nedostatečná autentizace	Neoprávněný přístup k datům: Změna dat	1	2	2	Mírné	
Nedostatečné fyzické zabezpečení	Krádež techniky s daty	2	3	6	Střední	Použití odpovídajících prostředků fyzické ochrany
Nedostatečné zálohování	Ztráta dat v případě selhání HW	2	3	6	Střední	Pravidelné zálohování
Zastaralost SW	Napadení malwarem	2	3	6	Střední	Používání aktuálního SW
Zastaralost SW	Nefunkčnost jiných SW prostředků	2	1	2	Mírné	
Zastaralost HW	Selhání HW: zničení dat	2	3	6	Střední	Pravidelná údržba
Zastaralost HW	Selhání HW: zničení techniky	1	2	2	Mírné	
Výpadek elektřiny	Nedostupnost technických prostředků	2	1	2	Mírné	

Případ č. 2

Zranitelnost	Hrozba	Pravděpodobnost	Dopad	Risk skóre	Riziko	Opatření ke snížení nebo eliminaci rizika
Nedostatečná autentizace	Neoprávněný přístup k datům: Krádež	1	3	3	Mírné	
Nedostatečná autentizace	Neoprávněný přístup k datům: Změna dat	1	2	2	Mírné	
Nedostatečné fyzické zabezpečení	Krádež techniky	2	2	4	Střední	Šifrování
Nedostatečné fyzické zabezpečení	Krádež techniky s daty	1	3	3	Mírné	
Nedostatečné zálohování	Ztráta dat v případě selhání HW	1	3	3	Mírné	
Nedostatečné zálohování	Ztráta konfigurace technických prostředků	1	2	2	Mírné	
Zastaralost SW	Napadení malwarem	1	3	3	Mírné	
Zastaralost SW	Nefunkčnost jiných SW prostředků	1	3	3	Mírné	
Zastaralost HW	Selhání HW: zničení dat	1	3	3	Mírné	
Zastaralost HW	Selhání HW: zničení techniky	1	3	3	Mírné	
Nedostatečně bezpečná síťová architektura	Neoprávněný přístup do sítě	2	2	4	Střední	Odpovídající zabezpečení přístupu do sítě
Nedostatečně bezpečná síťová architektura	Neoprávněný přístup k datům: Krádež nebo změna dat	2	3	6	Střední	Odpovídající zabezpečení sítě, Řízení přístupu uvnitř sítě

Nedostatečně bezpečná síťová architektura	Neoprávněný přístup k technice: Změna konfigurace	2	3	6 Střední	Odpovídající zabezpečení přístupu do sítě, Odpovídající zabezpečení prvků sítě
Nedostatečně bezpečná síťová architektura	Neoprávněný přístup k technice: Tiskárna			0	
Výpadek elektřiny	Nedostupnost technických prostředků	2	2	4 Střední	UPS

Případ č. 3

Zranitelnost	Hrozba	Pravděpodobnost	Dopad	Risk skóre	Riziko	Opatření ke snížení nebo eliminaci rizika
Nedostatečně bezpečná síťová architektura	Neoprávněný přístup do sítě: Vzdálený přístup	3	3	9 Vysoké		Firewall, Řízení přístupu
Nedostatečně bezpečná síťová architektura	Neoprávněný přístup k technice	1	3	3 Mírné		
Známé chyby v programech	Zneužití chyby útočníkem	1	1	1 Mírné		
Nedostatečné zálohování	Ztráta dat	1	3	3 Mírné		
Nedostatečné zálohování	Ztráta konfigurace technických prostředků	1	3	3 Mírné		
Nedostatečná identifikace a autentizace	Neoprávněný přístup k datům	1	3	3 Mírné		
Nedostatečná identifikace a autentizace	Neoprávněný přístup k technice	1	3	3 Mírné		
Špatná heslová politika	Prolomení hesel	2	3	6 Střední		Vynucování použití hesel odpovídající složitosti
Zastaralost SW	Nefunkčnost jiných SW prostředků	1	3	3 Mírné		
Neprokatelnost původu transakce	Neoprávněná změna dat	2	3	6 Střední		Řízení přístupu do informačního systému, logování
Nesprávný datum/čas	Konflikt - databáze, inf systém					
		2	3	6 Střední		Použití centrálního NTP serveru, použití serverového času
Nedostatečně odladěný program	Nefunkčnost některých operací	1	3	3 Mírné		
Chybné přiřazení přístupových práv	Neoprávněný přístup	2	3	6 Střední		Obezřetný proces přiřazování a kontroly oprávnění
Zneužití přiřazení přístupových práv	Útok interním útočníkem	2	3	6 Střední		
Nechráněné komunikační linky	Odposlech komunikace	1	3	3 Mírné		
Výpadek elektřiny	Nedostupnost technických prostředků	2	3	6 Střední		UPS
Sociální inženýrství	Vyzrazení autentizačních údajů	2	3	6 Střední		Školení