

Obsah

Úvod	9
1 Informace jako aktivum, pojmy a principy	13
1.1 Informace jako aktivum organizace	14
1.2 Další pojmy v bezpečnosti informací	15
1.3 Hodnota informací a cena jejich bezpečnosti	17
1.4 Bezpečnost informací jako proces	18
1.5 Stav bezpečnosti v českých firmách	19
1.6 Souhrnný příklad (1. kapitola) – definice a funkce příkladové organizace	25
2 Komplexní nebo dílčí řešení bezpečnosti	29
2.1 Tři kroky řešení	30
2.2 Studie informační bezpečnosti	32
2.3 Riziková analýza (analýza rizik) jako součást každého řešení	32
2.4 Bezpečnostní politika	34
2.5 Bezpečnostní projekt	35
2.6 Plány pro zvládání krizových situací	36
2.7 Souhrnný příklad (2. kapitola) – bezpečnostní politika, bezpečnostní projekt	40
3 Řízení bezpečnosti ve firmě nebo organizaci – bezpečnostní management	43
3.1 Nutnost existence bezpečnostní řídící struktury	44
3.2 Tři úrovně řízení bezpečnosti	45
3.3 První úroveň – bezpečnostní ředitel	47
3.4 Druhá úroveň – bezpečnostní specialisté	48
3.4.1 Bezpečnostní specialista pro personální bezpečnost	49
3.4.2 Bezpečnostní specialista pro administrativní bezpečnost	49
3.4.3 Bezpečnostní specialista pro objektovou a technickou bezpečnost	50

3.4.4 Bezpečnostní specialista pro bezpečnost informačních systémů	51
3.5 Třetí úroveň – bezpečnostní konzultanti	51
3.5.1 Název není důležitý	51
3.5.2 Dosažitelnost konzultantů	52
3.5.3 Funkce bezpečnostních konzultantů	52
3.6 Činnost bezpečnostního managementu při neobvyklých situacích	53
3.7 Souhrnný příklad (3. kapitola) – bezpečnostní management	54
4 Řešení a hodnocení bezpečnosti externí firmou nebo vlastními silami	55
4.1 Řešení bezpečnosti	56
4.2 Náklady na řešení bezpečnosti	58
4.3 Hodnocení bezpečnosti	60
4.3.1 Kritéria všeobecná a speciální	60
4.3.2 Standardní kritéria	60
4.3.3 Jednorázové hodnocení – audit	61
4.3.4 Průběžné hodnocení	63
4.4 Souhrnný příklad (4. kapitola) – interní či externí řešitel bezpečnosti	63
5 Bezpečnost informací a zákony	65
5.1 Ochrana osobních údajů	66
5.2 Pilíře ochrany firemních informací	66
5.3 Utajované skutečnosti	67
5.3.1 Zákon č. 148/1998 Sb. a utajované skutečnosti	67
5.3.2 Seznam utajovaných skutečností (vládní nařízení č. 246/1998 Sb. z 19. 10. 1998)	69
5.3.3 Další návazné předpisy k zákonu 148	70
5.3.4 Zajištění bezpečnosti podle zákona 148 – principy	71
5.3.5 Bezpečnostní prověrka organizace	75
5.4 Souhrnný příklad (5. kapitola) – bezpečnost informací vynucená zákony	76
6 Některé speciální případy s velkým dopadem na bezpečnost	79
6.1 Internet a Intranet	80
6.2 Elektronická pošta	82
6.3 Fax a telefon	83
6.4 EDI	84
6.5 Speciální způsoby ochrany informací – kryptografická ochrana (šifrování)	85
6.5.1 Cíl a použití	85

6.5.2 Šifrování se symetrickou šifrou.....	86
6.5.3 Šifrování s nesymetrickou šifrou.....	88
6.6 Elektronický podpis.....	90
6.7 Elektronický obchod a bankovní služby.....	93
6.8 Rok 2000 – opakování problému.....	93
6.9 Problémy spojené s evropskou integrací.....	94
6.10 Bezpečnost v kooperačních vztazích a subdodávkách.....	95
6.11 Antivirová ochrana.....	96
6.12 Souhrnný příklad (6. kapitola) – antivirová ochrana.....	97
7 Jak začít.....	99
7.1 Co máme za sebou.....	100
8 Závěr.....	105
9 Výsledky některých vybraných příkladů.....	109
9.1 Řešení příkladu z podkapitoly 1.6	
– definice a funkce příkladové organizace.....	110
9.2 Řešení příkladu z podkapitoly 2.7	
– bezpečnostní politika, bezpečnostní projekt.....	111
9.2.1 Obsah dokumentu CBP (celková bezpečnostní politika).....	112
9.2.2 Doplnkové otázky k celkové bezpečnostní politice.....	112
9.2.3 Správné odpovědi na doplňující otázky z podkapitoly 9.2.2.....	113
9.2.4 Obsah dokumentu SBP (systémová bezpečnostní politika).....	113
9.2.5 Doplnkové otázky k systémové bezpečnostní politice.....	113
9.2.6 Odpovědi na doplňující otázky z podkapitoly 9.2.5.....	114
9.2.7 Obsah dokumentu Bezpečnostní projekt fyzické ochrany prodejněho místa Králík, spol. s r.o., Olomouc.....	114
9.2.8 Doplnkové otázky k bezpečnostnímu projektu.....	115
9.2.9 Odpovědi na doplňující otázky z podkapitoly 9.2.8.....	115
9.3 Řešení příkladu z podkapitoly 3.7	
– bezpečnostní management.....	116
9.3.1 Formulář hlášení bezpečnostního incidentu.....	116
9.3.2 Doplnkové otázky k bezpečnostnímu managementu.....	116
9.3.3 Odpovědi na doplňující otázky z podkapitoly 9.3.2.....	118
9.4 Řešení příkladu z podkapitoly 4.4	
– řešení interním či externím řešitelem.....	118
9.4.1 Tým pro řešení objektové a technické bezpečnosti.....	118
9.4.2 Doplnkové otázky k řešení interním či externím řešitelem.....	119
9.4.3 Odpovědi na doplňkové otázky z pokapitoly 9.4.2.....	120
9.5 Řešení příkladu z podkapitoly 5.4	
– bezpečnost vynucená zákony.....	120
9.5.1 Seznam osob.....	120

9.5.2 Reakce na nový zákon	121
9.5.3 Informační systém	122
9.5.4 Doplnkové otázky k bezpečnosti vynucené zákony	122
9.5.5 Odpovědi na doplňkové otázky z podkapitoly 9.5.4	123
9.6 Řešení příkladu z podkapitoly 6.6 – antivirová ochrana	123
9.6.1 Koupit, či nikoliv	123
9.6.2 Co udělat jiného	124
9.6.3 Jaké ohrožení informací to přinese	124
9.6.4 Doplnkové otázky k některým speciálním problémům	125
9.6.5 Odpovědi na doplňkové otázky z podkapitoly 9.6.4.	126

10 Příloha A: Vybrané části z rizikové analýzy firmy Králík 127

10.1 Obsah dokumentu Závěry z rizikové analýzy Králík, spol. s r.o.	128
10.2 Struktura dokumentu Závěry z rizikové analýzy Králík, spol. s r.o.	128
10.3 Všeobecný popis bezpečnostní situace firmy Králík	129
10.4 Systém „Nákup stříbrných lišek“ (pro potřeby řešení příkladů)	130
10.4.1 Ohraničení zkoumaného systému	130
10.4.2 Umístění systému a jeho částí	130
10.4.3 IT	130
10.4.4 Komunikace	130
10.4.5 Správa systému	130
10.4.6 Vazba na další systémy	130
10.4.7 Bezpečnostní situace	131
10.4.8 Výstupy rizikové analýzy	133
10.4.9 Model systému	133
10.5 Splnění úkolu	133

11 Příloha B: Význam pojmů podle zákona č. 148/1998 Sb. a návazných vyhlášek 135

12 Literatura k dalšímu studiu 142