

OBSAH

Seznam zkratk.....	11
Úvod.....	15
Kapitola 1 Od bezpečnosti po kybernetickou bezpečnost.....	19
1.1 Bezpečnost jako neurčitý právní pojem	19
1.2 Prvky a systémy prvků kritické infrastruktury	21
1.3 Kybernetická bezpečnost	25
Kapitola 2 Legislativní východiska.....	33
2.1 Zákon o kybernetické bezpečnosti a související předpisy	33
2.2 Krizový zákon a prováděcí předpisy	34
2.3 Ochrana utajovaných informací	34
2.4 Další právní předpisy mající vztah k problematice bezpečnosti IS/IT	35
2.5 Právní předpisy EU.....	36
Kapitola 3 Útoky na IS/IT a jejich trestněprávní kvalifikace.....	38
3.1 Úmluva o počítačové kriminalitě a směrnice o útocích na informační systémy	38
3.2 Trestněprávní ochrana IS/IT podle trestního zákoníku	40
3.2.1 Trestné činy proti České republice, cizímu státu a mezinárodní organizaci.....	43
3.2.1.1 <i>Terorismus a kyberterrorismus</i>	44
3.2.1.2 <i>Sabotáž</i>	46
3.2.1.3 <i>Ohrožení utajované informace</i>	47
3.2.1.4 <i>Vyzvědačství</i>	49
3.2.2 Trestné činy obecně nebezpečné	50
3.2.2.1 <i>Obecné ohrožení</i>	51
3.2.2.2 <i>Poškození a ohrožení provozu obecně prospěšného zařízení</i>	52
3.2.3 Trestné činy proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství	54
3.2.3.1 <i>Neoprávněné nakládání s osobními údaji</i>	54
3.2.3.2 <i>Porušení tajemství dopravovaných zpráv</i>	58
3.2.4 Trestné činy proti průmyslovým právům a proti autorskému právu	62
3.2.5 Trestné činy proti majetku	62
3.2.6 Trestné činy proti počítačovému systému a nosiči informací ..	62
3.2.6.1 <i>Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230)</i>	64
3.2.6.1.1 <i>Skutková podstata podle odst. 1 a 2</i>	64

3.2.6.1.2	Skutková podstata podle odst. 3.....	69
3.2.6.1.3	Skutková podstata podle odst. 4.....	69
3.2.6.1.4	Skutková podstata podle odst. 5.....	70
3.2.6.2	Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231)	70
3.2.6.3	Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232).....	71
3.2.7	Další jednání pachatelů obtížně podřaditelná pod TrZ	73
Kapitola 4 Zákon o kybernetické bezpečnosti		75
4.1	Cíle zákona	75
4.2	Základní pojmy dle ZKB	79
4.3	Povinné subjekty dle ZKB	79
4.4	Určování povinných subjektů	82
4.4.1	Poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací dle § 3 písm. a) ZKB.....	82
4.4.2	Orgán nebo osoba zajišťující významnou síť dle § 3 písm. b) ZKB	82
4.4.3	Správce a provozovatel informačního nebo komunikačního systému kritické informační infrastruktury dle § 3 písm. c) a d) ZKB.....	83
4.4.4	Správce a provozovatel významného informačního systému dle § 3 písm. e) ZKB	85
4.4.5	Provozovatel základní služby nebo správce a provozovatel informačního systému základní služby dle § 3 písm. f) a g) ZKB	87
4.4.6	Poskytovatel digitální služby dle § 3 písm. h) ZKB.....	94
4.5	Povinnosti určených orgánů a osob (§ 4–4a).....	96
4.5.1	Bezpečnostní opatření.....	96
4.5.2	Smlouvy s poskytovatelem služeb cloud computingu.....	98
4.5.3	Nepřímá novela zákona o veřejných zakázkách v § 4	98
4.5.4	Vztahy mezi správcí a provozovatelem podle § 4a.....	110
4.6	Bezpečnostní opatření podle § 5 ZKB	111
4.6.1	Organizační opatření (§ 5 odst. 2)	111
4.6.2	Technická opatření (§ 5 odst. 3).....	112
4.7	Vyhláška o kybernetické bezpečnosti dle Směrnice NIS.....	113
4.7.1	Vymezení pojmů (§ 2)	114
4.7.2	Systém řízení bezpečnosti informací (§ 3).....	115
4.7.3	Řízení aktiv (§ 4)	117
4.7.4	Řízení rizik (§ 5).....	119
4.7.5	Organizační bezpečnost (§ 6).....	121

4.7.6	Řízení dodavatelů (§ 8).....	129
4.7.7	Bezpečnost lidských zdrojů (§ 9)	136
4.7.8	Řízení provozu a komunikací (§ 10).....	141
4.7.9	Řízení změn (§ 11)	142
4.7.10	Řízení přístupu (§ 12)	144
4.7.11	Akvizice, vývoj a údržba (§ 13)	147
4.7.12	Zvládání kybernetických bezpečnostních událostí a incidentů (§ 14)	148
4.7.13	Řízení kontinuity činností (§ 15)	148
4.7.14	Audit kybernetické bezpečnosti (§ 16).....	161
4.7.15	Fyzická bezpečnost (§ 17)	164
	4.7.15.1 <i>Technická opatření</i>	166
	4.7.15.2 <i>Režimová opatření</i>	166
	4.7.15.3 <i>Fyzická ostraha</i>	167
4.7.16	Bezpečnost komunikačních sítí (§ 18)	167
4.7.17	Správa a ověřování identit (§ 19).....	171
4.7.18	Řízení přístupových oprávnění (§ 20)	175
4.7.19	Ochrana před škodlivým kódem (§ 21)	175
4.7.20	Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů (§ 22)	177
4.7.21	Detekce kybernetických bezpečnostních událostí (§ 23)	180
4.7.22	Sběr a vyhodnocování kybernetických bezpečnostních událostí (§ 24)	181
4.7.23	Aplikační bezpečnost (§ 25)	183
	4.7.23.1 <i>Black-box testy</i>	184
	4.7.23.2 <i>White-box testy</i>	184
	4.7.23.3 <i>Grey-box testy</i>	184
4.7.24	Kryptografické prostředky (§ 26).....	188
4.7.25	Zajišťování úrovně dostupnosti informací (§ 27)	190
4.7.26	Průmyslové, řídicí a obdobné specifické systémy (§ 28).....	193
4.7.27	Digitální služby (§ 29)	198
4.7.28	Bezpečnostní politika a bezpečnostní dokumentace (§ 30) ...	201
	4.7.28.1 <i>Bezpečnostní politika</i>	201
	4.7.28.2 <i>Obsah bezpečnostní dokumentace</i>	207
4.8	Vztahy mezi správcí a provozovateli podle § 6a ZKB.....	209
4.9	Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident (§ 7 a § 8 ZKB, § 14, § 31 a § 32 vyhlášky).....	210
4.9.1	Hlášení kybernetického bezpečnostního incidentu	211
4.9.2	Kategorizace kybernetických bezpečnostních incidentů	213
4.9.3	Forma a náležitosti hlášení kybernetických bezpečnostních incidentů	214
4.10	Opatření a jiné úkony podle ZKB (§ 11–15a).....	217

4.10.1	Opatření (§ 11)	217
4.10.2	Varování (§ 12)	218
4.10.3	Reaktivní opatření (§ 13 ZKB a § 33 vyhlášky).....	219
4.10.4	Opatření obecné povahy (§ 14–15a ZKB)	220
4.11	Národní úřad pro kybernetickou a informační bezpečnost	222
4.11.1	Úřad, jeho poslání a činnosti (§ 21a–22c ZKB)	222
4.11.2	Evidence kybernetických bezpečnostních incidentů (§ 9–10a)	225
4.11.3	Národní CERT (§ 17–19 ZKB).....	226
4.11.4	Vládní CERT (§ 20 ZKB)	229
4.11.5	Stav kybernetického nebezpečí (§ 21 ZKB).....	230
4.11.6	Kontrola v oblasti kybernetické bezpečnosti a nápravná opatření (§ 23–24)	232
4.11.7	Kontrola činnosti Úřadu (§ 24a–24b)	234
Kapitola 5 Normy, standardy a metodiky pro bezpečnost IS/IT		236
5.1	Od bezpečnostních politik k normám a standardům.....	236
5.2	Použitá terminologie	237
5.3	České organizace pro standardizaci	237
5.4	Mezinárodní organizace pro standardizaci	239
5.4.1	ISO, IEC.....	239
5.4.2	NIST, ANSI, BSI	240
5.4.3	ISACA.....	240
5.5	Standardizace IS a IT v oblasti bezpečnosti informací	240
5.6	Vývoj standardů pro hodnocení bezpečnosti informací	241
5.6.1	TCSEC	242
5.6.2	OECD	245
5.6.3	CTCPEC.....	245
5.6.4	FC.....	246
5.6.5	ITSEC.....	246
5.6.6	Společná kritéria (Common Criteria – CC)	247
5.6.7	ČSN ISO/IEC 15408	249
5.6.8	Standardy ISO.....	250
	5.6.8.1 <i>Organizační struktura ISO</i>	250
	5.6.8.2 <i>Standardy ISO vydávané SC 27</i>	251
	5.6.8.3 <i>Technické normy ČSN ISO/IEC řady 27000</i>	254
	5.6.8.4 <i>ISO/IEC 20000</i>	259
	5.6.8.5 <i>ISO/IEC 9000</i>	260
5.7	Technické standardy	260
5.7.1	FIPS 140-2	260
5.7.2	Další normy ČSN ISO/IEC	262
5.8	Metodiky	263
5.8.1	COBIT	263
	5.8.1.1 <i>Principy COBIT® 2019</i>	264

5.8.1.2	<i>Cíle správy a řízení (Management objectives)</i>	265
5.8.1.3	<i>Komponenty systému governance (Components of a governance system)</i>	266
5.8.1.4	<i>Oblasti zaměření (Focus areas)</i>	267
5.8.1.5	<i>Faktory návrhu (Design factors)</i>	267
5.8.1.6	<i>Kaskádování cílů (Goal cascade)</i>	267
5.8.1.7	<i>Implementace systému</i>	268
5.8.2	ITIL	268
5.8.3	SSAE-16.....	271
5.8.4	PCI DSS	273
Kapitola 6 Řízení bezpečnosti informací		274
6.1	Business model ISACA	275
6.2	Metodiky řízení bezpečnosti informací	277
6.2.1	COBIT	278
6.2.2	ITIL 4	279
6.2.3	ISO/IEC 27002 (ČSN ISO/IEC 27002).....	281
6.2.4	Porovnání COBIT 5, ITIL 4 a ISO/IEC 27002	282
6.3	Návrh systému řízení bezpečnosti informací	282
6.3.1	Postup při návrhu systému řízení bezpečnosti informací	287
6.3.2	Začlenění ISMS do struktury organizace.....	290
Kapitola 7 Řízení rizik		294
7.1	Definice pojmů.....	294
7.1.1	Aktivum.....	294
7.1.2	Hrozba	295
7.1.3	Zranitelnost.....	296
7.1.4	Opatření	296
7.1.5	Riziko	297
7.2	Řízení rizik jako proces.....	300
7.3	Řízení rizik a aktiv podle § 4–5 vyhlášky č. 82/2018 Sb.	303
7.3.1	Proces řízení rizik podle § 5 vyhlášky	303
7.3.2	Proces řízení aktiv podle § 4 vyhlášky.....	304
7.3.3	Příloha č. 1 vyhlášky – Hodnocení aktiv.....	306
7.3.4	Příloha č. 2 vyhlášky – Hodnocení rizik	307
7.3.5	Příloha č. 3 – Příklady zranitelností a hrozeb.....	308
7.4	Analýza rizik.....	309
7.4.1	Identifikace aktiv	310
7.4.2	Stanovení hodnoty a seskupování aktiv	310
7.4.3	Identifikace hrozeb.....	310
7.4.4	Analýza hrozeb a zranitelností	311
7.4.5	Ztráta.....	311
7.4.6	Metody analýzy rizik.....	312
7.4.6.1	<i>Kvalitativní metody</i>	312
7.4.6.2	<i>Kvantitativní metody</i>	313

7.4.6.3	<i>Kombinované metody</i>	313
7.4.7	Volby strategie analýzy rizik	313
7.4.8	Příklad metod pro analýzu rizik.....	314
Kapitola 8	Trestní odpovědnost fyzických a právnických osob	319
8.1	Úvod	319
8.2	Přestupky dle § 25 ZKB.....	321
8.2.1	Odpovědnost právnické osoby za přestupek.....	334
8.2.2	Odpovědnost podnikající fyzické osoby za přestupek	338
8.3	Trestní odpovědnost za porušení povinností uložených ZKB	339
8.4	Trestní odpovědnost právnické osoby	348
Kapitola 9	Občanskoprávní aspekty bezpečnosti IS/IT, povinnost předcházet škodám, odpovědnost za škodu	356
Závěr	362	
Summary	364	
Literatura	365	
O autorech	369	
Věcný rejstřík	371	