Předmluva vydavatele 5

Předmluva autorů 9

Seznam zkratek 25

I Základní terminologie 33

1 Kyberprostor (Cyberspace) 35

2 Pojem kybernetické bezpečnosti a pojmy související 39
2.1 Kybernetická bezpečnost 39
2.2 Principy kybernetické bezpečnosti 45
2.2.1 Triáda CIA 45
2.2.2 Prvky kybernetické bezpečnosti 56
2.2.3 Životní cyklus kybernetické bezpečnosti 63
2.3 Riziko, aktivum, zranitelnost 68
2.3.1 Riziko 68
2.3.2 Aktivum 72
2.3.3 Zranitelnost 72
2.4 Kybernetické hrozby, události, incidenty a útoky 73
2.4.1 Kybernetická hrozba 74
2.4.2 Kybernetická bezpečnostní událost 80
2.4.3 Kybernetický (bezpečnostní) incident 81
2.4.4 Kybernetický útok (Cyber Attack) 82
2.4.5 Kyberkriminalita (Cybercrime) 83

II Legislativa 85

3 Legislativní základ kybernetické bezpečnosti 87
3.1 Legislativní vývoj kybernetické bezpečnosti v ČR 87
3.2 Právní normy vztahující se ke kybernetické bezpečnosti 94
3.2.1 Dokumenty EU/ES sloužící k harmonizaci právních úprav při řešení problematiky kybernetické bezpečnosti 95
3.2.2 Právní normy ČR 98
3.3 Exkurze do práv a povinností vyplývajících z některých právních norem 99
3.3.1 GDPR 101
3.3.1.1 Místní působnost GDPR 104
3.3.1.2 Osobní údaj 104

3.3.1.3 Zpracování osobních údajů 109
3.3.1.4 Zabezpečení osobních údajů 111
3.3.1.5 Posouzení vlivu na ochranu osobních údajů (DPIA) 112
3.3.2 ePrivacy 113
3.3.2.1 Působnost ePrivacy 114
3.3.2.2 Základní terminologie ePrivacy 115
3.3.2.3 Zpracování dat 118
3.3.3 Občanský zákoník 120
3.3.3.1 Ochrana soukromí 121
3.3.3.2 Právní jednání 123
3.3.3.3 Náhrada škody 123
3.3.4 Trestní zákoník 124

4 Zákon o kybernetické bezpečnosti 129
4.1 Příčiny vzniku ZoKB 130
4.2 Základní cíle a principy ZoKB 133
4.3 Komentář k ZoKB 138
§ 1 Předmět úpravy 138
§ 2 Vymezení pojmů 142
Kybernetický prostor 148
Kritická informační infrastruktura 150
Bezpečnost informací 154
Významný informační systém 154
Správce informačního systému 164
Správce komunikačního systému 164
Provozovatel informačního nebo komunikačního systému 164
Významná síť elektronických komunikací 167
Základní služba. Informační systém základní služby. 167
Provozovatel základní služby 189
Digitální služba 197
Příslušný orgán 198
§ 3
Poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací 200
Orgán nebo osoba zajišťující významnou síť 205
Správce a provozovatel informačního systému kritické informační infrastruktury 208
Správce a provozovatel komunikačního systému kritické informační infrastruktury 208
Správce a provozovatel významného informačního systému 216
Správce a provozovatel informačního systému základní služby 222

Provozovatel základní služby 228
Poskytovatel digitální služby 233
§ 3a Zástupce poskytovatele digitálních služeb 237
§ 4 Bezpečnostní opatření 241
§ 4a 248
§ 5 250

Organizační opatření 253
Systém řízení bezpečnosti informací 253
Řízení rizik 259
Bezpečnostní politika 264
Organizační bezpečnost 266
Stanovení bezpečnostních požadavků pro dodavatele 274
Řízení aktiv 275
Bezpečnost lidských zdrojů 276
Řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému 277
Řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému 277
Akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů 278
Zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů 279
Řízení kontinuity činností 280
Kontrola a audit kritické informační infrastruktury a významných informačních systémů 281

Technická opatření 281
Fyzická bezpečnost 282
Nástroj pro ochranu integrity komunikačních sítí 285
Nástroj pro ověřování identity uživatelů 285
Nástroj pro řízení přístupových oprávnění 287
Nástroj pro ochranu před škodlivým kódem 288
Nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů 289
Nástroj pro detekci kybernetických bezpečnostních událostí 290
Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí 291
Aplikační bezpečnost 292
Kryptografické prostředky 292
Nástroj pro zajišťování úrovně dostupnosti informací 293
Bezpečnost průmyslových a řídicích systémů 294

§ 6 294
§ 6a 295
§ 7 Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident 299
§ 8 Hlášení kybernetického bezpečnostního incidentu 302
§ 9 Evidence 311
§ 10 314
§ 10a 316
§ 11 Opatření 319
§ 12 Varování 323
§ 13 Reaktivní a ochranné opatření 325
§ 14 330
§ 15 331
§ 15a 334
§ 16 Kontaktní údaje 335
§ 17 Národní CERT 340
§ 18 Provozovatel národního CERT 348
§ 19 Veřejnoprávní smlouva 353
§ 20 Vládní CERT 356
§ 21 Stav kybernetického nebezpečí 361
§ 21a Úřad 367
§ 22 367
§ 22a Určení provozovatele základní služby a informačního systému základní služby 374
§ 22b 379
§ 23 Kontrola 381
§ 24 Nápravná opatření 384
§ 24a Kontrola činnosti Úřadu 386
§ 24b 388
§ 24c 388
§ 25 Přestupky 389
§ 26 393
§ 27 Společné ustanovení k přestupkům 394
§ 28 Zmocňovací ustanovení 394
§ 29 Přechodná ustanovení 395
§ 30 396
§ 31 397
§ 32 398
§ 33 Společná ustanovení 399
§ 35 Změna zákona o elektronických komunikacích 401
§ 37 Změna zákona o provozování rozhlasového a televizního vysílání 402
§ 38 Účinnost 402

III Kyberbezpečnost prakticky **405**

5 Fyzická bezpečnost **411**
5.1 Zajištění perimetru 411
5.2 Kontrola přístupu 412
5.3 Vnitřní bezpečnost 415
5.4 Ochrana počítačových systémů 416
5.4.1 Opatření proti krádeži počítačových systémů 417
5.4.2 Ochrana před rozebráním a úpravou počítačových systémů 418
5.4.3 Ochrana před připojením cizích periferií k počítačovým systémům 420

6 Bezpečnost sítí a služeb **425**
6.1 Ochrana sítí 425
6.1.1 Rozdělení sítě jako základní prvek zajištění bezpečnosti 426
6.1.1.1 DMZ 426
6.1.1.2 VLAN 427
6.1.2 Ochrana sítě LAN 429
6.1.2.1 DHCP protokol 429
6.1.2.2 ARP protokol 431
6.1.2.3 DNS 435
6.1.2.4 IEEE 802.1X 438
6.1.2.5 Bezdrátové sítě 439
6.1.2.6 IPv6 451
6.1.3 Ochrana na rozhraní sítí 455
6.1.3.1 Access Control List (ACL) 455
6.1.3.2 Firewall 455
6.1.3.3 Proxy server 458
6.1.3.4 Intrusion Detection System (IDS) a Intrusion Prevention System (IPS) 460
6.1.3.5 Security Information and Event Management (SIEM) 461
6.1.3.6 Antivir, Antispam 462
6.2 Aplikační bezpečnost 462
6.2.1 Řízení přístupů 462
6.2.2 Ověřování uživatelů 463
6.2.3 Hesla 464
6.2.4 Logy a logování 475
6.2.5 Zabezpečení důvěrnosti a integrity přenášených dat 476
6.2.6 Zranitelnosti 478
6.3 Ochrana koncových počítačových systémů 480
6.4 Vzdálený přístup k počítačovým systémům 481
6.5 Paměťová média 484
6.6 Správa a dohled nad počítačovou sítí 485

6.7 Přenosné počítačové systémy 487
6.8 Bezpečnost lidských zdrojů 489
6.9 Reakce na incident 490
6.9.1 Hlášení bezpečnostních incidentů 492
6.9.2 Interní hlášení bezpečnostních incidentů 492
6.9.3 Řešení bezpečnostních incidentů 493
6.10 Možnosti využití dalších informačních zdrojů o incidentech 495
6.10.1 Malicious Domain Manager 496
6.10.2 Cyber Threat Intelligence Project - PROKI 497

7 CERT/CSIRT týmy 505
7.1 Historie 505
7.2 CERT a CSIRT týmy 506
7.3 Jak vzniká CERT/CSIRT tým 508
7.4 Spolupráce CERT/CSIRT infrastruktury 510
7.5 Hierarchie CERT/CSIRT týmů? 512
7.6 Národní a vládní CERT/CSIRT týmy 513
7.7 Situace v ČR a ve světě 514
7.8 Národní CSIRT České republiky 515
7.9 Vládní CERT České republiky 516
7.10 Na který CERT/CSIRT tým se obrátit? 516

Závěr 519

Seznam použitých pramenů a dalších zdrojů 523

Rejstřík 541

Summary 560