

OBSAH

PŘEDMLUVA	9
1. ÚVOD	11
1.1 ZÁKLADNÍ NÁZVOSLOVÍ	12
1.2 ZÁKLADNÍ POJMY	12
1.3 DEFINICE ISMS	14
1.4 ZÁKLADNÍ POJMY A NÁZVOSLOVÍ INFORMAČNÍ BEZPEČNOSTI	15
1.4.1 Pojmy	15
1.4.2 Ustavení ISMS	16
1.4.3 Zavádění a provoz ISMS	17
1.4.4 Monitorování a přezkoumání ISMS	17
1.4.5 Údržba a zlepšování ISMS	17
1.4.6 Blokový diagram procesů při zavádění ISMS	18
2. HISTORIE	21
3. DEMINGŮV MODEL	27
3.1 PDCA	28
4. DEFINICE POJMŮ	31
4.1 ITIL®	32
4.2 COBIT®	35
4.3 CRAMM	40
4.4 RAMSES	41
4.5 COMMON CRITERIA – CC	42
4.6 PŘIMĚŘENÁ BEZPEČNOST	45
5. NORMALIZAČNÍ INSTITUCE	47
5.1 POJMY	48
5.2 NADNÁRODNÍ, CELOSVĚTOVÉ	49
5.3 EVROPSKÉ	50
5.4 NÁRODNÍ	51
5.5 DALŠÍ	52
5.5.1 Další evropské normalizační/standardizační organizace zabývající se bezpečností IT	52
5.5.2 Americké normalizační (standardizační) organizace zabývající se bezpečností IT	53

6. NORMY	55
6.1 ZÁKLADNÍ NORMY ŘADY 27 k	56
6.2 CHYSTANÉ NORMY ŘADY 27 k	68
6.3 TELEKOMUNIKAČNÍ PROSTŘEDÍ	69
6.4 ENERGETIKA	70
6.5 ZDRAVOTNICKÉ PROSTŘEDÍ	70
6.6 SÍŤOVÁ BEZPEČNOST	71
6.7 SOUVISEJÍCÍ NORMY S ŘADOU ISO 27 k	73
7. ZAVÁDĚNÍ ISMS	79
7.1 OBSAH ISMS	80
7.2 ETAPY ZAVÁDĚNÍ ISMS	80
7.3 POVINNÁ DOKUMENTACE	82
7.4 ŠKOLENÍ	84
7.5 MĚŘENÍ ÚČINNOSTI	85
7.6 MONITOROVÁNÍ A AUDITY	87
8. PROJEKTOVÁNÍ ISMS	89
8.1 BEZPEČNOSTNÍ PROJEKT	90
9. AKTIVA	95
9.1 DEFINICE A KLASIFIKACE AKTIV	96
9.2 HODNOCENÍ AKTIV	96
9.3 VÝPOČET HODNOTY AKTIVA	97
9.4 ZRANITELNOST AKTIVA	98
10. BEZPEČNOSTNÍ HROZBY	99
10.1 MODEL SÍŤOVÝCH HROZEB	102
11. ANALÝZA RIZIK	109
11.1 METODIKY	111
11.2 ŘÍZENÍ RIZIK	115
12. BEZPEČNOSTNÍ OPATŘENÍ	119
12.1 DEFINICE	120
12.2 VÝBĚR OPATŘENÍ	121
12.3 USPOŘÁDÁNÍ OPATŘENÍ	123
12.4 PŘEHLED OPATŘENÍ	126
12.5 MAPOVÁNÍ ISO/IEC 27002:2022 NA ISO/IEC 27002:2013	136
13. AUDIT A CERTIFIKACE	141
13.1 ZÁKLADNÍ POJMY	142
13.2 PRŮBĚHY PROCESŮ	143

14. EKONOMICKÁ STRÁNKA ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI	145
15. ZABEZPEČENÍ A OCHRANA DAT	149
15.1 POJMY	150
15.2 KRYPTOLOGIE	151
15.3 VIRY A ŠKODLIVÉ KÓDY	153
15.4 IDS A IPS	154
15.5 DLP SYSTÉMY	158
16. SÍŤOVÁ BEZPEČNOST	161
16.1 DEFINICE A POJMY	162
16.2 NORMY	163
16.3 VRSTVY ISO/OSI MODELU (L1, L2, L3)	168
16.4 MANAGEMENT BEZPEČNOSTI PASIVNÍ VRSTVY	169
16.5 BUDOVÁNÍ BEZPEČNÉ SÍŤOVÉ INFRASTRUKTURY	172
16.6 SHODA S NORMOU ISO/IEC 27002:2020	173
17. APLIKAČNÍ BEZPEČNOST	177
17.1 DEFINICE A POJMY	178
17.2 NORMY	179
17.3 BEZPEČNOST APLIKAČNÍ VRSTVY	181
17.4 BEZPEČNOST WEBOVÝCH APLIKACÍ	182
18. PRŮMYSLOVÁ BEZPEČNOST	185
18.1 VYMEZENÍ POJMŮ	186
18.2 INDUSTRIAL ETHERNET (IE)	188
18.3 PARAMETRY PRŮMYSLOVÉ SÍŤOVÉ INFRASTRUKTURY	189
18.4 TOPOLOGIE	190
18.5 REDUNDANCE	194
18.6 SCADA	199
18.7 SYNCHRONIZACE V DISTRIBUOVANÝCH ŘÍDICÍCH SYSTÉMECH	200
18.8 NORMY BEZPEČNOSTI V PRŮMYSLOVÉM PROSTŘEDÍ	202
19. OBOROVÉ ISMS	207
19.1 ISMS VE STÁTNÍ SPRÁVĚ	208
19.1.1 Pojmy a definice	208
19.1.2 Právní prostředí	209
19.1.3 Normy a směrnice	212
19.1.4 Kritická opatření	214
19.2 ISMS VE ZDRAVOTNICTVÍ	215
19.2.1 Definice	215
19.2.2 Provozní a právní prostředí	216
19.2.3 Normy	218
19.3 ISMS A POSKYTOVATELÉ ICT SLUŽEB	223

19.3.1	Pojmy	223
19.3.2	Bezpečnostní stavební bloky ITU-T	225
19.3.3	Normy	226
19.3.4	Konvergence k NGN	229
19.4	ISMS V ENERGETICE	232
19.4.1	Pojmy	233
19.4.2	Bezpečnostní výzvy	233
19.4.3	Řízení informační (kybernetické) bezpečnosti	234
19.4.4	Normy	235
19.5	ISMS V DOPRAVĚ	239
19.5.1	Princip konceptu bezpečnosti	240
19.5.2	Normy	241
19.6	ISMS V AKADEMICKÉM PROSTŘEDÍ	243
20.	SPECIFICKÉ ŘEŠENÍ ISMS	251
20.1	SCADA	252
20.1.1	Definice	252
20.1.2	Standardizace	254
20.1.3	Bezpečnost SCADA	255
20.2	DATOVÉ CENTRUM – DC	257
20.2.1	Definice a pojmy	257
20.2.2	Studie proveditelnosti	258
20.2.3	Předpokládaná struktura hrozeb	265
20.2.4	Provoz datového centra	266
20.2.5	Normy pro DC	268
20.2.6	Kategorizace DC	269
20.2.7	Certifikace DC	270
20.2.8	Zelená DC	271
20.3	REDUNDANCE HW	272
20.3.1	Pojmy	272
20.3.2	Princip HW redundance	273
20.4	BEZPEČNOST ÚLOŽIŠŤ DAT	278
20.4.1	Pojmy	278
20.4.2	Zabezpečení datových úložišť	280
20.4.3	Normy	280
20.4.4	Problematika datových úložišť	281
20.4.5	Správa datových úložišť	281
20.4.6	Zelená datová úložiště	282
21.	ITSM	285
21.1	POJEM ITSM	286
21.2	SPECIFIKACE SLUŽEB V SLA	287
21.3	NORMA ISO/IEC 20000	288
21.4	NORMA ISO/IEC 27013	294

22. PŘÍPADOVÉ STUDIE	297
22.1 METODIKA PRAKTICKÉHO ZAVEDENÍ ISMS	298
22.2 SOFTWAREVÝ NÁSTROJ PRO GARANTY INFORMAČNÍCH AKTIV ESKO-KB	299
22.3 ANALÝZA RIZIK	304
22.3.1 Identifikace a hodnocení aktiv	304
22.3.2 Identifikace hrozeb a zranitelností	304
22.3.3 Maticová metoda analýzy rizik	305
22.3.4 Analýza rizik pomocí pravděpodobnosti incidentu a jeho dopadu	307
22.3.5 Srovnávací (GAP) analýza rizik	309
22.4 POUŽITÍ FUNKCE FILTROVÁNÍ PRO NÁPRAVNÁ OPATŘENÍ DLE ISO/IEC 27002:2022	310
22.5 VÝBĚR OPATŘENÍ A JEJICH MĚŘENÍ	313
22.6 METODIKA A NÁVRH BEZPEČNÉ INFRASTRUKTURY IT	316
22.7 SÍŤOVÁ BEZPEČNOST DLE ISO/IEC 27033	318
22.8 ZABEZPEČENÍ SÍŤOVÉ INFRASTRUKTURY	324
22.8.1 Metodika zabezpečení síťové infrastruktury	324
22.8.2 Aplikace síťových opatření	328
22.9 SEGMENTACE SÍŤE DLE ISO/IEC 27002:2022	330
22.10 ŘÍZENÍ PŘÍSTUPU	331
22.11 FUNKČNÍ MODEL NAC	337
22.12 KLASIFIKACE FIREWALLŮ	352
22.13 UTM – KOMPLEXNÍ OCHRANA	359
22.14 TOPOLOGICKÁ STUDIE SÍŤE V PRŮMYSLOVÉM PROSTŘEDÍ	361
22.14.1 Popis	361
22.14.2 Topologie hvězda	361
22.14.3 Topologie kruh	363
22.14.4 Vyhodnocení	364
22.15 VÝPOČET DOSTUPNOSTI	365
22.16 BEZPEČNOST BEZDRÁTOVÉHO ŘEŠENÍ	367
22.16.1 Historie bezpečnosti WiFi	367
22.16.2 Kategorie útoků na bezdrátové sítě a možnosti obrany	367
22.16.3 Autentizační metody ve WiFi 6	369
22.16.4 Zranitelnosti WiFi 6	370
22.16.5 Doporučení WiFi Aliance	371
22.17 METODIKA ZÁLOHOVÁNÍ DAT	371
22.17.1 Záloha a archiv	372
22.17.2 Privátní zálohování třetí stranou	380
22.18 ANTIVIROVÉ DESATERO	382
22.19 UŽIVATEL JAKO ZDROJ RIZIK	384
22.20 BEZPEČNOSTNÍ SMĚRNICE PRO UŽIVATELE LAN A IS	386
22.20.1 Forma dokumentu „Minimální bezpečnostní pravidla pro uživatele“	388

22.20.2	Příklad provozního řádu počítačové sítě (školy)	391
22.20.3	Bezpečnostní školení	394
23.	REJSTRÍK OBECNĚ POUŽÍVANÝCH POJMŮ	395
24.	PŘEHLED VYBRANÝCH AKTUÁLNÍCH A RELEVANTNÍCH BEZPEČNOSTNÍCH NOREM ŘADY 27 K	405
25.	SEZNAM ZKRATEK	409
26.	SEZNAM OBRÁZKŮ	415
27.	SEZNAM TABULEK	419
28.	POUŽITÁ LITERATURA	421