OBSAH

Autorský kolektiv **9**

Předmluva **11**

Úvod **13**

1 Integrovaný systém řízení **19**

1.1 Model PDCA 21

1.2 Řízení rizik 23

1.3 Systém řízení kvality – QMS 23

1.4 Systém řízení vztahu k okolí – EMS 24

1.5 Systém řízení bezpečnosti a ochrany zdraví při práci – OHASMS 25

2 Řízení informatiky a bezpečnosti informací v organizaci **27**

2.1 Vývoj řízení informatiky v organizacích 27

2.2 Koncepce řízení informatiky 30

2.2.1 IT Governance – ITG 30

2.2.2 IT Service Management – ITSM 34

2.3 Information Security Governance – ISG 36

2.3.1 Business model pro bezpečnost informací 40

2.4 Metodiky 42

2.4.1 COBIT 42

2.4.2 ITIL 48

2.4.3 Porovnání metodik ITIL a COBIT 52

3 Metodiky řízení bezpečnosti informací **55**

3.1 Vymezení bezpečnosti informací 55

3.2 Historický vývoj 60

3.2.1 Trusted Computer Security Evaluation Criteria 62

3.2.2 Information Technology Security Evaluation Criteria 63

3.2.3 Canadian Trusted Computer Product Evaluation Criteria 65

3.2.4 Federal Criteria 66

3.3 Porovnání kritérií hodnocení bezpečnosti 66

3.4 Common Criteria – CC 68

3.4.1 Obecný model hodnocení 69

3.4.2 Požadavky na bezpečnostní funkce 71

3.4.3 Požadavky na záruky 72

3.5 Normalizace řízení bezpečnosti informací 75

3.5.1 Historie normalizace řízení bezpečnosti informací 75

3.5.2 Řada ISO/IEC 27000 – Řízení bezpečnosti informací 78

4 Systém řízení bezpečnosti informací 85
4.1 Ustanovení ISMS 86
4.1.1 Definice rozsahu a hranic ISMS 87
4.1.2 Prohlášení o politice ISMS 88
4.1.3 Pravidla a postupy řízení rizik 90
4.1.4 Souhlas vedení se zavedením ISMS a se zbytkovými riziky 100
4.1.5 Prohlášení o aplikovatelnosti 101
4.1.6 Shrnutí etapy ustanovení ISMS 102
4.2 Zavádění a provoz ISMS 104
4.2.1 Plán zvládaní rizik 104
4.2.2 Příručka bezpečnosti informací 105
4.2.3 Prohlubování bezpečnostního povědomí 106
4.2.4 Měření účinnosti ISMS 106
4.2.5 Řízení provozu, zdrojů, dokumentace a záznamů ISMS 116
4.3 Monitorování a přezkoumání ISMS 117
4.3.1 Provádění kontrol ISMS 117
4.3.2 Interní audity ISMS 118
4.3.3 Přezkoumání ISMS vedením organizace 118
4.4 Udržba a zlepšování ISMS 119
4.4.1 Soustavné zlepšování ISMS 120
4.4.2 Odstraňování nedostatků ISMS 120
4.5 Shrnutí celého cyklu ISMS 121
4.6 Praktická doporučení 122
4.7 Výhled na rok 2012 123
5 Realizace bezpečnostních opatření 125
5.1 Bezpečnostní politika 127
5.2 Organizace bezpečnosti informací 127
5.2.1 Organizační struktury 129
5.2.2 Organizace řízení bezpečnosti – příklady 131
5.3 Řízení aktiv 135
5.3.1 Klasifikace informací 136
5.4 Bezpečnost z hlediska lidských zdrojů 140
5.5 Fyzická bezpečnosti a bezpečnost prostředí 141
5.6 Řízení komunikací a řízení provozu 143
5.7 Řízení přístupu 145
5.7.1 Principy řízení přístupu 146
5.8 Akvizice, vývoj a údržba informačních systémů 147
5.9 Zvládání bezpečnostních incidentů 148
5.9.1 Principy zvládání bezpečnostních incidentů 148
5.9.2 Životní cyklus SIMS 150
5.9.3 Organizační struktury a odpovědnosti spojené s řešením bezpečnostních incidentů 155

5.9.4 Podpora mezinárodními normami ... 156
5.10 Řízení kontinuity činností organizace ... 157
5.10.1 Mezinárodní přístupy k řízení kontinuity ... 158
5.10.2 Specifické požadavky na řízení kontinuity ICT ... 163
5.10.3 Obecný postup obnovy chodu činností ... 165
5.10.4 Praktická doporučení pro budování BCMS ... 167
5.11 Soulad s požadavky ... 169
5.12 Výhled na rok 2012 ... 170

6 Audit a testování bezpečnosti informací ... 173

6.1 Základy auditu bezpečnosti ... 174
6.1.1 Principy auditu ... 174
6.1.2 Postup auditu ... 175
6.1.3 Základní typy auditů ... 177
6.1.4 Kvalifikace auditorů ... 178
6.2 Certifikace systému řízení bezpečnosti informací ... 179
6.2.1 Certifikace versus akreditace ... 179
6.2.2 Průběh certifikace ISMS ... 181
6.2.3 Údržba a obnova certifikátu ... 182
6.3 Techniky pro provádění testů bezpečnosti informací ... 182

7 Úřady, instituce a organizace zabývající se bezpečností informací ... 185

7.1 Právní rámec bezpečnosti informací v České republice ... 185
7.1.1 Strategie kybernetické bezpečnosti ... 205
7.2 Tuzemské instituce ... 206
7.2.1 Úřad pro ochranu osobních údajů – ÚOOÚ ... 206
7.2.2 Národní bezpečnostní úřad – NBÚ ... 208
7.2.3 Ministerstvo vnitra – MV ČR, Odbor koncepce a koordinace ISVS ... 210
7.2.4 Český normalizační institut – ČNI ... 214
7.2.5 Úřad pro technickou normalizaci, metrologii a státní zkušebnictví – ÚNMZ ... 214
7.2.6 Český institut pro akreditaci – ČIA ... 217
7.2.7 Český telekomunikační úřad – ČTÚ ... 219
7.3 Evropské instituce ... 219
7.3.1 British Standards Institute – BSI ... 220
7.3.2 Bundesamt für Schicherheit in der Informationstechnik – německý BSI ... 220
7.3.3 European Network and Information Security Agency – ENISA ... 220
7.3.4 Evropský institut telekomunikačních norem – ETSI ... 221
7.3.5 Evropská komise pro normalizaci – CEN ... 221
7.3.6 Vládní úřad pro obchod – OGC ... 221
7.4 Ostatní instituce ... 222
7.4.1 Americký národní normalizační institut – ANSI ... 222
7.4.2 Asociace pro audit a řízení informačních systémů – ISACA ... 222
7.4.3 Institute of Electrical and Electronics Engineers – IEEE ... 223

7.4.4 International Electrotechnical Commission – IEC 223
7.4.5 Internet Engineering Task Force – IETF 223
7.4.6 Mezinárodní organizace pro normalizaci – ISO 224
7.4.7 Národní institut pro normy a technologie – NIST 228
7.4.8 National Security Agency – NSA 228
7.4.9 RSA Laboratories – standardy PKCS 228

8 Trendy a vývoj bezpečnosti informací 231
8.1 Stav bezpečnosti informací v České republice 231
8.1.1 Hlavní zjištění 233
8.1.2 Dílčí zjištění 233
8.1.3 Celkové zhodnocení 240
8.2 Trendy v bezpečnosti informací a v bezpečnosti IS/ICT 241
8.2.1 Trendy v České republice 241
8.2.2 Světové a evropské trendy 243

Závěr 245

Summary 247

Příloha – Intergovaný systém řízení – IMS – Podrobnosti 249

Použitá literatura a další zdroje 267

Seznam obrázků a tabulek 281

Rejstřík 283