

OBSAH

PŘEDMLUVA	9
ÚVOD.....	11
1 VÝCHODISKA ŘÍZENÍ KYBERNETICKÉ BEZPEČNOSTI A BEZPEČNOSTI INFORMACÍ	17
1.1 Vymezení kybernetické bezpečnosti	17
1.2 Vymezení bezpečnosti informací	21
1.3 Vztah kybernetické bezpečnosti a bezpečnosti informací	27
1.4 Manažerský princip PDCA a integrovaný systém řízení.....	29
1.4.1 Princip PDCA.....	31
1.4.2 Aplikace principu PDCA pro systém řízení bezpečnosti informací	33
1.5 Normalizace řízení bezpečnosti informací	34
1.5.1 Historie normalizace řízení bezpečnosti informací	34
1.5.2 Řada ISO/IEC 27000 – Řízení bezpečnosti informací	37
2 KYBERNETICKÁ BEZPEČNOST V ČESKÉ REPUBLICĚ.....	49
2.1 Regulační rámec kybernetické bezpečnosti.....	50
2.1.1 Směrnice NIS	50
2.1.2 Provozovatel základních služeb	50
2.1.3 Poskytovatel digitálních služeb.....	52
2.1.4 Výjimky	54
2.1.5 Další úkoly ze Směrnice NIS.....	54
2.2 Agentura ENISA	55
2.2.1 Kyber balíček.....	55
2.3 Vznik kybernetického zákona v České republice.....	56
2.3.1 Strategie pro oblast kybernetické bezpečnosti České republiky 2012–2015	57
2.3.2 Rada pro kybernetickou bezpečnost.....	57
2.4 Zákon o kybernetické bezpečnosti	58
2.4.1 Související právní předpisy.....	60
2.4.2 Národní strategie kybernetické bezpečnosti České republiky 2015–2020 ...	63
2.5 Role Národního úřadu pro kybernetickou a informační bezpečnost	65
2.5.1 Bezpečnostní týmy.....	65
2.5.2 Stav kybernetického nebezpečí.....	68
2.6 Povinné subjekty podle zákona o kybernetické bezpečnosti	69
2.6.1 Poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací	69
2.6.2 Orgány nebo osoby zajišťující významnou síť	70

2.6.3	<i>Správci a provozovatelé kritické informační infrastruktury a systémů základních služeb</i>	70
2.6.4	<i>Správci a provozovatelé významného informačního systému (VIS)</i>	73
2.6.5	<i>Poskytovatelé digitálních služeb</i>	74
2.7	Požadovaná bezpečnostní opatření.....	75
2.7.1	<i>Požadavky vyhlášky o kybernetické bezpečnosti</i>	76
2.7.2	<i>Organizační opatření</i>	76
2.7.3	<i>Technická opatření</i>	85
2.7.4	<i>Bezpečnostní politika a bezpečnostní dokumentace</i>	87
2.7.5	<i>Hlášení kontaktních údajů</i>	88
2.7.6	<i>Hlášení kybernetických bezpečnostních incidentů</i>	88
3	SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ	89
3.1	Kontext organizace.....	90
3.1.1	<i>Porozumění organizaci a jejímu kontextu</i>	91
3.1.2	<i>Porozumění potřebám a očekávání zainteresovaných stran</i>	91
3.1.3	<i>Stanovení rozsahu systému řízení bezpečnosti informací</i>	92
3.1.4	<i>Systém řízení bezpečnosti informací</i>	93
3.2	Vůdčí role kybernetické bezpečnosti a bezpečnosti informací.....	94
3.2.1	<i>Vůdčí role a závazek</i>	94
3.2.2	<i>Politika kybernetické bezpečnosti a bezpečnosti informací</i>	95
3.2.3	<i>Role, odpovědnosti a pravomoci organizace</i>	96
3.3	Rizika a cíle kybernetické bezpečnosti a bezpečnosti informací.....	97
3.3.1	<i>Opatření zaměřená na rizika a příležitosti</i>	97
3.3.2	<i>Cíle kybernetické bezpečnosti a bezpečnosti informací</i>	125
3.4	Podpora kybernetické bezpečnosti a bezpečnosti informací.....	127
3.4.1	<i>Zdroje</i>	128
3.4.2	<i>Kompetence</i>	128
3.4.3	<i>Povědomí</i>	135
3.4.4	<i>Komunikace</i>	136
3.4.5	<i>Dokumentované informace</i>	136
3.5	Provozování kybernetické bezpečnosti a bezpečnosti informací.....	137
3.5.1	<i>Plánování a řízení provozu</i>	137
3.5.2	<i>Posouzení rizik kybernetické bezpečnosti a bezpečnosti informací</i>	139
3.5.3	<i>Ošetření rizik kybernetické bezpečnosti a bezpečnosti informací</i>	139
3.6	Hodnocení výkonnosti kybernetické bezpečnosti a bezpečnosti informací.....	139
3.6.1	<i>Monitorování, měření, analýza a hodnocení ISMS</i>	140
3.6.2	<i>Interní audity ISMS</i>	152
3.6.3	<i>Přezkoumání ISMS vedením organizace</i>	159
3.7	Zlepšování systému řízení kybernetické bezpečnosti a bezpečnosti informací..	161

3.7.1	<i>Neshody a nápravná opatření</i>	161
3.7.2	<i>Neustálé zlepšování</i>	162
3.8	Shrnutí řízení kybernetické bezpečnosti a bezpečnosti informací.....	162
3.8.1	<i>Praktická doporučení</i>	165
3.9	Výhled na rok 2020+.....	166
4	REALIZACE OPATŘENÍ KYBERNETICKÉ BEZPEČNOSTI A BEZPEČNOSTI INFORMACÍ	167
4.1	Politiky bezpečnosti informací.....	169
4.2	Organizace bezpečnosti informací	171
4.2.1	<i>Organizační struktury</i>	173
4.2.2	<i>Organizace řízení bezpečnosti – příklady</i>	175
4.2.3	<i>Mobilní zařízení a práce na dálku</i>	179
4.3	Bezpečnost lidských zdrojů.....	180
4.4	Řízení aktiv	181
4.4.1	<i>Klasifikace informací</i>	183
4.4.2	<i>Použití klasifikace informací</i>	187
4.5	Řízení přístupu	189
4.5.1	<i>Principy řízení přístupu</i>	192
4.6	Kryptografie	193
4.7	Fyzická bezpečnosti a bezpečnost prostředí.....	194
4.8	Bezpečnost provozu	196
4.9	Bezpečnost komunikací.....	200
4.10	Akvizice, vývoj a údržba informačních systémů.....	201
4.10.1	<i>Metodika Vývoj – Bezpečnost – Provoz (DevSecOps)</i>	205
4.10.2	<i>Příklad kategorizace vývoje</i>	206
4.11	Vztahy s dodavateli	207
4.11.1	<i>Příklad kategorizace dodavatelů</i>	209
4.12	Řízení incidentů bezpečnosti informací	209
4.12.1	<i>Principy zvládnání bezpečnostních incidentů</i>	210
4.12.2	<i>Životní cyklus SIMS</i>	212
4.12.3	<i>Organizační struktury a odpovědnosti spojené s řešením bezpečnostních incidentů</i>	219
4.12.4	<i>Podpora mezinárodními normami</i>	220
4.13	Řízení kontinuity činností organizace	221
4.13.1	<i>Mezinárodní přístupy k řízení kontinuity činností</i>	223
4.13.2	<i>Specifické požadavky na řízení kontinuity ICT</i>	229
4.13.3	<i>Obecný postup obnovy chodu činností</i>	231
4.13.4	<i>Praktická doporučení pro budování BCMS</i>	234

4.14	Soulad s požadavky	236
4.14.1	<i>Řízení ochrany soukromí</i>	<i>238</i>
4.15	Sektorové výklady	238
4.15.1	<i>Řízení bezpečnosti informací pro telekomunikační organizace</i>	<i>239</i>
4.15.2	<i>Řízení bezpečnosti informací pro cloudové služby</i>	<i>240</i>
4.15.3	<i>Řízení bezpečnosti informací pro energetický průmysl.....</i>	<i>241</i>
4.15.4	<i>Řízení bezpečnosti informací pro loterijní a herní organizace</i>	<i>242</i>
4.16	Výhled na rok 2021/2022	243
ZÁVĚR.....		245
SUMMARY.....		247
SEZNAM TABULEK		249
SEZNAM OBRÁZKŮ.....		251
LITERATURA A DALŠÍ ZDROJE		253
REJSTŘÍK.....		267