

Obsah

Profil autora.....	7
Předmluva	9
1. Význam bezpečnosti informací.....	10
2. Řízení přístupu k informacím.....	13
2.1 Význam řízení přístupu k informacím.....	13
2.2 Techniky řízení přístupu k informacím	15
2.2.1 Rozdělení technik řízení přístupu k informacím.....	15
2.2.2 Technika přenechání volnému uvážení.....	15
2.2.3 Techniky nepřenechání volnému uvážení.....	15
2.3 Administrace řízení přístupu	18
2.3.1 Význam administrace řízení přístupu	18
2.3.2 Správa uživatelských účtů	18
2.3.3 Zaznamenávání aktivity uživatelů	18
2.3.4 Řízení přístupových práv	18
3. Autentizace.....	20
3.1 Autentizace a její základní dělení.....	20
3.2 Další dělení autentizace	21
3.3 Znalostní autentizace	22
3.4 Autentizace prostřednictvím autentizačního předmětu	23
3.5 Biometrická autentizace	23
3.6 Kvantitativní ukazatele autentizace	25
4. Škodlivý kód	30
4.1 Malware.....	30
4.2 Počítačový virus	30
4.3 Počítačový červ	31
4.4 Spam.....	32
4.5 Hoax	32
4.6 Logická bomba	33
4.7 Trojský kůň.....	33
4.8 Adware	33
4.9 Keylogger	34
4.10 Hijacker	34
4.11 Dialer	34

4.12 Sniffer.....	34
4.13 Spyware.....	34
4.14 Samotný informační systém.....	34
5. Útoky, monitoring a sociotechniky.....	35
5.1 Útoky.....	35
5.2 Monitoring.....	39
5.2.1 Význam monitoringu.....	39
5.2.2 Systémy pro detekci útoků.....	39
5.2.3 Související nástroje.....	41
5.2.4 Penetrační testy.....	41
5.3 Sociotechniky.....	41
5.3.1 Zneužití sociotechnik.....	41
5.3.2 Sociotechnický cyklus.....	43
5.3.3 Faktory usnadňující sociotechnický útok a varovné příznaky.....	43
5.3.4 Příklad sociotechnického útoku.....	44
6. Kryptologie.....	45
6.1 Kryptologie, kryptografie a kryptoanalýza.....	45
6.2 Princip kryptografie.....	45
6.3 Dělení šifrovacích algoritmů.....	46
6.4 Symetrické šifrovací algoritmy.....	47
6.4.1 Princip symetrických šifrovacích algoritmů.....	47
6.4.2 Caesarova šifra.....	47
6.4.3 Vigenèrova šifra.....	48
6.4.4 Vernamova šifra.....	48
6.4.5 Moderní symetrické šifrovací algoritmy.....	49
6.5 Asymetrické šifrovací algoritmy.....	49
6.5.1 Princip asymetrických šifrovacích algoritmů.....	49
6.5.2 Moderní asymetrické šifrovací algoritmy.....	50
6.6 Kryptoanalýza.....	50
6.6.1 Útok hrubou silou.....	50
6.6.2 Frekvenční kryptoanalýza.....	50
7. Elektronický podpis.....	52
7.1 Princip elektronického podpisu.....	52
7.2 Infrastruktura veřejného klíče.....	53

7.3	Zaručený elektronický podpis	54
8.	Fyzická bezpečnost	55
8.1	Význam fyzické bezpečnosti	55
8.2	Program fyzické bezpečnosti	55
8.2.1	Cíle programu fyzické bezpečnosti	55
8.2.2	Tvorba programu fyzické bezpečnosti	56
8.2.3	Metriky měření efektivity bezpečnostních mechanismů	56
8.3	CPTED	56
8.3.1	Význam CPED	56
8.3.2	Základní strategie CPTED	57
8.4	Volba polohy budov	57
8.5	Konstrukce budov	58
8.6	Vstupní body budovy	58
8.7	Okna	58
8.8	Ochrana před zcizením notebooků	59
8.9	Trezory	59
8.10	Poruchy elektrické sítě	59
8.11	Záložní zdroj energie	60
8.12	Ochrana před statickou elektřinou	61
8.13	Detektory požáru	61
8.14	Bezpečnostní kamerové systémy	62
9.	Analýza rizik	63
9.1	Význam analýzy rizik	63
9.2	Druhy analýzy rizik	64
9.3	Kvantitativní analýza rizik	64
9.4	Kvalitativní analýza rizik	65
9.5	Porovnání kvantitativní a kvalitativní analýzy rizik	66
9.6	Nakládání s rizikem	67
10.	Plánování řízení bezpečnosti	68
10.1	Řízení bezpečnosti	68
10.2	Bezpečnostní politiky	68
10.3	Bezpečnostní standardy	70
10.4	Bezpečnostní normy	71

10.5 Bezpečnostní postupy	71
10.6 Bezpečnostní procedury	71
11. Řízení bezpečnosti a zaměstnanci.....	72
11.1 Životní cyklus zaměstnance	72
11.2 Bezpečnostní role	73
12. Plánování kontinuity podnikových procesů (BCP)	75
12.1 Význam BCP	75
12.2 Postup BCP	75
12.2.1 Stanovení rozsahu projektu BCP	75
12.2.2 Ohodnocení významu podnikových procesů (BIA)	76
12.2.3 Tvorba BCP	77
12.2.4 Schválení a implementace BCP	78
12.3 Dokumentace BCP	78
13. Plánování obnovy po pohromě (DRP)	79
13.1 Význam DRP	79
13.2 Strategie DRP	79
13.2.1 Komunikace v případě pohromy	79
13.2.2 Změna pracovní lokality	80
13.2.3 Zálohování, skladování, přenos a obnova dat	81
13.3 Tvorba DRP	82
13.4 Školení a dokumentace DRP	82
13.5 Testování a správa DRP	83
14. Počítačová kriminalita	84
Literatura	86
Seznam zkratk	87
Seznam obrázků	89
Seznam tabulek.....	89