

# Obsah

Předmluva

1

Kapitola 1

## Lehký úvod do počítačové bezpečnosti **3**

1.1 Kryptologie	4
1.1.1 Symetrická kryptografie	5
1.1.2 Asymetrická kryptografie	5
1.2 Ochrana dat	6
1.3 Autentizace a řízení přístupu	8
1.3.1 Autentizační protokoly	8
1.3.2 Útoky na autentizační protokoly	9
1.3.3 Řízení přístupu	10
1.4 Digitální podpis	10
1.4.1 Certifikáty veřejného klíče	12
1.5 Bezpečná síť	12
1.5.1 Ochrana přenášených dat	13
1.5.2 Ochrana připojených počítačů	14
1.6 Škodlivý software	15
1.6.1 Antiviry	16
1.7 Normy a certifikace	17
1.7.1 Hodnocení bezpečnosti IT	18
1.8 Útoky a útočníci	19
1.9 Bezpečná firma	21
1.10 Jak dál?	22

Kapitola 2

## Kryptologie **23**

2.1 Úvod do kryptografie	24
2.1.1 Symetrická versus asymetrická kryptografie	25
2.1.2 Šifrování nebo podepisování?	27

2.1.3	Proudové a blokové šifry	28
2.2	Útoky na kryptografické algoritmy	31
2.2.1	Útok hrubou silou	31
2.2.2	Luštění se znalostí šifrovaného textu	32
2.2.3	Luštění se znalostí otevřeného textu	32
2.2.4	Luštění se znalostí vybraných otevřených textů	32
2.2.5	Luštění se znalostí vybraných šifrových textů	33
2.2.6	Luštění pomocí kompromitace uživatelů	33
2.2.7	Nároky kladené na šifrovaný text	33
2.3	Symetrická kryptografie	34
2.3.1	Substituční šifry	34
2.3.2	Nerozlučitelná šifra	38
2.3.3	Transpoziční šifry	38
2.3.4	Šifrovací algoritmus DES	39
2.3.5	Šifrovací algoritmus AES	41
2.3.6	Další symetrické algoritmy	42
2.4	Asymetrická kryptografie	42
2.4.1	Váhy a zavazadla	43
2.4.2	Algoritmus RSA	44
2.4.3	Další algoritmy veřejných klíčů	45

### Kapitola 3

## Ochrana dat

**47**

3.1	Auditní záznam	49
3.1.1	Obsah auditního záznamu	50
3.1.2	Analýza auditních záznamů	51
3.2	Ochrana fyzického přístupu k nosičům dat	52
3.2.1	Omezení přístupu	53
3.2.2	Ochrana před katastrofami	54
3.2.3	Zálohované napájení	55
3.3	Ochrana logického přístupu k datům	56
3.3.1	Identifikace, autentizace a řízení přístupu	56
3.3.2	Praktické tipy	57
3.4	Ochrana uložených dat	57
3.5	Ochrana dat přenášených počítačovou sítí	59
3.5.1	Ochrana před modifikací	60

3.5.2	Ochrana před kompromitací	60
3.6	Ochrana dat před zničením	61
3.6.1	Zálohování	61
3.6.2	Práce se záložními kopiemi	62
3.6.3	Obnova ze záloh	62
3.6.4	Duplikace	63

## Kapitola 4

# **Autentizace a řízení přístupu** **65**

4.1	Získání autentizační informace od uživatele	66
4.1.1	Důkaz znalostí	66
4.1.2	Důkaz vlastnictvím	67
4.1.3	Důkaz vlastností	68
4.2	Obvyklé útoky na autentizační protokoly	69
4.2.1	Útok opakováním (replay attack, eavesdropping attack)	69
4.2.2	Útok ze středu (man-in-the-middle attack)	70
4.2.3	Útok na hesla (password attack)	70
4.2.4	Útok na integritu zpráv (integrity attack)	71
4.3	Návrh autentizačního protokolu	71
4.3.1	Slabé autentizační metody	71
4.3.2	Jednorázová hesla	72
4.3.3	Časové razítkování	72
4.3.4	Metoda výzva-odpověď	73
4.3.5	Důvěryhodná třetí strana	74
4.4	Moderní autentizační protokoly	74
4.4.1	Autentizace ve Windows NT verze 4	74
4.4.2	Autentizační protokol Kerberos	75
4.4.3	RADIUS	75
4.4.4	Autentizace v SSL	75
4.4.5	Autentizace v sítích GSM	76
4.5	Řízení přístupu	76
4.5.1	Přístup ke zdrojům a objektům v systému	77
4.5.2	Přístup ke zdrojům	77
4.5.3	Přístup k objektům	78
4.5.4	Nepovinné řízení přístupu	79
4.5.6	Skryté kanály v systémech MAC	80

6.4	Firewally	116
6.4.1	Rozdělení firewallů	116
6.4.2	Personální firewally	120
6.4.3	Umístění firewallu	120
6.4.4	Single Point of Failure	122
6.5	Základní bezpečnostní pravidla	123
6.5.1	Antivirová ochrana	123
6.5.2	Ochrana proti spamu	124
6.5.3	Ochrana proti hackerům	125
6.5.4	Ochrana proti odposlechu	126

## Kapitola 7

# Škodlivý software 127

7.1	Základní dělení – viry a ti další	128
7.2	Destrukční činnost škodlivého software	128
7.3	Virus a červ pod lupou	129
7.3.1	Viry šířící se pomocí boot sektoru	129
7.3.2	Viry šířící se pomocí spustitelných souborů	130
7.3.3	Viry šířící se pomocí nespustitelných souborů	132
7.3.4	Červi šířící se pomocí počítačových sítí	133
7.3.5	Některé techniky používané při tvorbě virů	135
7.4	Jak pracuje antivirus	136
7.4.1	Vyhledávání virů na základě signatur	136
7.4.2	Vyhledávání virů na základě heuristické analýzy	137
7.4.3	Další metody vyhledávání virů	137
7.5	Moderní antivirové systémy	138

## Kapitola 8

# Normy a certifikace 141

8.1	Bezpečnostní normy	141
8.1.1	De facto standardy	143
8.2	Certifikáty shody	143
8.3	Hodnocení bezpečnosti IT	144
8.3.1	Jak probíhá certifikace	144
8.4	Významná kritéria pro hodnocení bezpečnosti	145

8.4.1	TCSEC	146
8.4.2	ITSEC	148
8.4.3	CTCPEC	150
8.4.4	Common Criteria	151

**Kapitola 9****Útoky a útočníci 153**

9.1	Nebezpečnost útočníků	155
9.1.1	Amatéři	155
9.1.2	Hackeři	155
9.1.3	Profesionálové	155
9.2	Hackeři a crackeři	156
9.2.1	Cracker	156
9.2.2	Hacker	156
9.3	Pasivní útoky	157
9.4	Aktivní zasahování do komunikace	159
9.5	Útoky na dostupnost služeb	160
9.5.1	DoS, dDoS	161
9.6	Útoky na převzetí moci	163
9.6.1	Fyzický přístup k počítači	163
9.6.2	Vzdálený přístup k počítači	163
9.6.3	Útok na spuštěné programy	163

**Kapitola 10****Bezpečná firma 165**

10.1	Personální zajištění bezpečnosti	166
10.1.1	Chief Information Security Officer – CISO	167
10.2	Bezpečnostní politika firmy	168
10.2.1	Definice základních pojmů	139
10.2.2	Analýza rizik	170
10.2.3	Identifikace aktiv	170
10.2.4	Identifikace hrozeb	171
10.2.5	Vlastní analýza rizik	172
10.2.6	Navržení vhodné ochrany	172
10.2.7	Havarijní plány	173

10.2.8	Uložení bezpečnostní politiky	176
10.3	Personální a administrativní bezpečnost	177
10.3.1	Životní cyklus zaměstnance	177
10.3.2	Školení zaměstnanců	180
10.3.3	Směrnice a nařízení	181

## Kapitola 11

# **Závěrem**

**183**

---

## Kapitola 12

# **Další vhodná literatura**

**185**

---

# **Rejstřík**

**187**

---