

Obsah

Pár slov úvodem	11
Co se v knize dozvíte	13

Kapitola 1

Základy počítačových sítí	17
Typy sítí	17
Hub, switch a adresování	18
Odposlouchávání při použití hubu	19
Pár slov o síti Ethernet	20
Připojení počítače do sítě	20
Síťová konfigurace počítače	21
Příkazy ping, pathping a ipconfig	22
Pracovní skupiny	25
Přidání počítače do pracovní skupiny	26
Zobrazení počítačů dostupných v pracovní skupině	26
Aplikace VisualRoute 2006 Personal	27
Základní funkce a možnosti programu	27
Získání údajů o dostupnosti vzdáleného počítače	28
Detailní popis síťové cesty	29
Zjišťování dalších detailů	30
Bezpečnostní politika	30
Optimistický přístup	31
Liberální přístup	31
Paranoidní přístup	31

Kapitola 2

Rozdíly mezi Windows XP Home a Professional	33
Síťové funkce	33
Doménové účty	33
SNMP a IPSec	34
Internet Information Services	34
Ochrana dat	34
Šifrování souborů a složek	34
Zálohování	34
Přístupová práva	35

Kapitola 3

Bez Service Packu 2 ani krok	37
Stažení a instalace Service Packu 2	37
Co Service Pack 2 přináší	39
Další bezpečnostní podpora společnosti Microsoft	39
Nástroj pro odstranění škodlivého softwaru	39
Microsoft Baseline Security Analyzer	40
Přehled možností po prvním spuštění	41
Kontrola bezpečnosti počítače	41

Kapitola 4

Centrum zabezpečení	45
Brána firewall	46
Filtrování paketů	46
Konfigurace Brány firewall systému Windows	47
Automatické aktualizace	49
Webová služba Windows Update	51
Aktualizace ostatního softwaru	51
Ochrana proti virům	52

Kapitola 5

Místní uživatelské účty a skupiny	53
Vytvoření uživatelského účtu	54
Výchozí uživatelské účty systému Windows	54
Volba Uživatelské účty v Ovládacích panelech	54
Přidání nového účtu pomocí příkazu net user	55
Úprava existujícího uživatelského účtu	56
Místní uživatelé a skupiny	56
Microsoft Management Console	57
Správa uživatelských účtů příkazem net accounts	58

Kapitola 6

Ochrana a bezpečnost dat	61
Nástroj Zálohování	61
Průvodce vytvořením záloh nástrojem Zálohování	61
Nástroj Obnovení systému a body obnovení	64
Vytvoření bodu obnovení	65
Použití vytvořených bodů obnovení	65
Šifrování dat pomocí Windows	67
Souborové systémy FAT, FAT32 a NTFS	67
Šifrování souborů a složek	67
Externí aplikace pro zálohování dat zdarma	69

File Backup Watcher Free Edition	69
SyncBack Freeware	71
TrueCrypt	76
Stažení a instalace češtiny	76
Vytvoření šifrovaného disku	77
Označení šifrované jednotky	79
Možnosti práce s šifrovanou jednotkou	80
Ucelený přehled softwaru dostupného zdarma	81
Cryptainer LE	81
File Backup Watcher Free Edition	81
FineCrypt	82
Simply Safe Backup	82
SyncBack Freeware	82
TrueCrypt	82

Kapitola 7

Síťové zdroje a jejich zabezpečení	83
Rozdíl mezi zjednodušeným a klasickým sdílením	83
Zjednodušené sdílení složky	83
Klasické sdílení	84
Nové sdílení složky	84
Nastavení oprávnění	85
Sdílení tiskáren	86
Nové sdílení tiskárny	86
Nastavení oprávnění	87
Přístup ke sdíleným zařízením a datům	88
Místa v síti	88
Připojení síťové jednotky	88
Příkaz net use	89

Kapitola 8

Zabezpečení internetového připojení	91
Nastavení síťového připojení v Internet Exploreru	91
Připojení prostřednictvím místní sítě	91
Nastavení parametrů proxy-serveru	92
Nastavení bezpečnosti Internet Exploreru	92
Zóny zabezpečení	93
Další možnosti ochrany citlivých informací	97
Práce s certifikáty v prohlížeči Internet Explorer	101
Přehled možností	101
Kontrola certifikátu serveru při připojení	102
Import a export certifikátů	103
Anonymní surfování	104

Stručný úvod do principu proxy-serverů	104
Webové anonymizéry	104
Anonymizační aplikace	107
ArchiCrypt Stealth	108
Internet Sweeper	109
Základní přehled možností a nastavení	110
Výběr údajů určených k odstranění	111
Cookie Monster	112
Základní možnosti a funkce programu	112
Jednoduchá správa cookies	113
Volby nastavení	114
Úprava chování Internet Exploreru pomocí registru	115
Mazání dočasně uložených souborů	115
Odstranění ikon v panelu nástrojů	115
Omezení možností nastavení	116
Odstranění hesla funkce hodnocení obsahu	117
Zabránění v přístupu k lokálním složkám	117

Kapitola 9

Ochrana osobním firewallem	119
ZoneAlarm	119
Prvotní konfigurace	119
Možnosti a význam nabídek	120
Nastavení zón a úrovní bezpečnosti	121
Pravidla pro síťová spojení aplikací	122
Sunbelt Kerio Personal Firewall	125
Režimy Simple a Advanced	125
Přehled obsahu a funkcí Sunbelt Kerio Personal Firewall	125
Automatické přidání nového pravidla	127
Přidání pravidla paketového filtru	128
Blokování chování aplikací	129
McAfee Personal Firewall Plus	131
Přehled základních funkcí	131
Automatické přidání a správa pravidel	132
Možnosti nastavení bezpečnosti	134
Přehled osobních firewallů zdarma	135
Adorons Firewall	135
Agnitum Outpost Firewall	135
Filseclab Personal Firewall Professional Edition	135
Jetico Personal Firewall	135
Sunbelt Kerio Personal Firewall	136
SoftPerfect Personal Firewall	136
ZoneAlarm	136

Kapitola 10

Ochrana proti počítačovým virům	137
Preventivní ochrana proti škodlivému kódu	137
1. Pravidelně zálohujte	137
2. Dávejte pozor na data z cizích zdrojů a e-mailových příloh	138
3. Používejte specializované aplikace a pravidelně je aktualizujte	139
4. Používejte firewall	139
5. Nepanikařte	139
Klasické počítačové viry	140
Možnosti antivirových aplikací	140
Antivirové programy	141
Avast! 4 Home Edition	141
NOD32	146
Programy pro detekci a odstranění trojských koní	149
Anti-Trojan Shield	150
The Cleaner	152
Software pro detekci rootkitů	155
RootkitRevealer	156
BlackLight Beta	156
Přehled a odkazy na související aplikace	158
Anti-Trojan Shield	158
Avast! 4 Home Edition	158
AVG Anti-Virus	158
BlackLight Beta	158
Kaspersky Anti-Virus Personal	158
McAfee VirusScan	158
NOD32	158
Norton AntiVirus 2006	159
RootkitRevealer	159
The Cleaner	159

Kapitola 11

Spyware	161
Možnosti a varianty spywaru	161
Adware	161
Browser hijackery	161
Keyloggery	162
Cookies	162
Základní možnosti obrany proti spywaru	162
Základní přehled o aktuálně běžících procesech	162
Automaticky spouštěné programy	164
Zásady bezpečného surfování	164
Antispywarové produkty zdarma	165

Ad-Aware SE Personal Edition	165
Spybot Search & Destroy	167
Obrana proti browser hijackerům a dialerům zdarma	170
HijackThis	170
Mrsoft Antidialer	172
Správa automaticky spouštěných aplikací a běžících procesů	173
Nástroj pro konfiguraci systému	173
Příkazy tasklist a taskkill	174
CodeStuff Starter	176
Stav nouze	177
Přehled souvisejících aplikací dostupných zdarma	178
Ad-Aware SE Personal Edition	178
CodeStuff Starter	178
HijackThis	178
Mrsoft Antidialer	178
Process Explorer	178
Spybot Search & Destroy	178
SpywareBlaster	179
What's Running	179

Kapitola 12

Spam (nevyžádaná pošta)	181
Spim	181
Chraňte svou e-mailovou adresu	181
Jak spammeři získávají vaše adresy	182
Automatické blokování odesílatelů	183
Hodnocení obsahu e-mailu	183
Ochrana před nevyžádanou poštou v aplikaci Outlook Express	184
Přidání uživatele mezi blokové odesílatele	184
Změna a odebrání blokových odesílatelů	185
Ochrana před nevyžádanou poštou v aplikaci Mozilla Thunderbird	185
Základní možnosti nastavení ochrany	185
Aktivace a použití Bayesova filtru	187
Spamihilator	187
Instalace aplikace a její základní nastavení	187
Instalace češtiny	188
Správa černých a bílých listin	189
Podporované filtry	190
Výukový filtr	192
Cactus Spam Filter	193
Výuka filtru	194
Detekce a odstranění nevyžádané pošty	195
ChoiceMail Free	197
Prvotní nastavení	198

Odmítnutí odesílatelů a potvrzení identity	198
McAfee SpamKiller 2006	200
Základní přehled funkcí a možností	200
Přidání uživatelů a domén mezi přátele	201
Práce se spamovými zprávami	203
Nastavení základních možností filtrování	203
Globální filtry	205
Vytvoření nového filtru	206
Přehled softwaru dostupného zdarma	207
Cactus Spam Filter	207
ChoiceMail Free	207
SpamBayes	207
Spamihilator	207
SpamPal	207
Závěr v podobě shrnutí bezpečnostních zásad	209
Rozmyslete si, kterou verzi Windows XP potřebujete	209
Pravidelně aktualizujte veškerý software	209
Používejte dostatečně silná hesla	209
Šifrujte a zálohujte	209
Dbejte na zabezpečení sdílených prostředků	210
Surfujte bezpečně	210
Nedejte šanci počítačovým virům	210
Chraňte se proti spywaru	210
Nedejte šanci spamu	210
Příloha	
Slovníček pojmů	211
Rejstřík	213