Obsah

Úvod ..... *xv*

I: ZÁKLADY POČÍTAČOVÉ BEZPEČNOSTI *1*

1: Úvod *3*

Co je to počítačová bezpečnost? 6

Co je to operační systém? 7

Historie Unixu 8

Unix a bezpečnost 15

Úloha této knihy 20

2: Strategie a doporučení *23*

Plánování bezpečnostních potřeb 24

Odhad rizika 27

Analýza poměru nákladů a efektu 30

Strategie 35

Bezpečnost a zatemňování 40

II: ZODPOVĚDNOST UŽIVATELŮ *47*

3: Uživatelé a hesla *49*

Uživatelská jména 49

Hesla 51

Zadávání hesla 57
Změna hesla 58
Ověření nového hesla 59
Volba hesla 61
Jednorázová hesla 6
Shrnutí 68

4: Uživatelé, skupiny a superuživatel 71
Uživatelé a skupiny 71
Speciální uživatelská jména 78
su: Změna identity 84
Shrnutí 90

5: Souborový systém Unixu 91
Soubory 91
Použití přístupových práv 100
umask 113
Použití přístupových práv adresářů 115
SUID 118
Soubory zařízení 129
chown: Změna vlastníka souboru 132
chgrp: Změna skupiny souboru 134
Neobvyklé a nedobré nápady 134
Shrnutí 137

6: Kryptografie 139
Stručná historie kryptografie 139
Co je to šifrování? 142
Šifrovací systém Enigma 147
Obvyklé šifrovací algoritmy 149
Výtahy zpráv a digitální podpisy 167
Šifrovací programy na Unixu 174
des: Data Encryption Standard 178
Šifrování a zákonné úpravy v USA 190

III: BEZPEČNOST SYSTÉMU 195

7: Zálohy 197

Zálohujte! 198
Příklady zálohovacích strategií 210
Zálohování systémových souborů 215
Zálohovací software 218

8: Ochrana účtů 225

Nebezpečné účty 225
Sledování formátu souborů 235
Omezení přihlášení 236
Správa nevyužívaných účtů 237
Ochrana superuživatelského účtu 243
Systém šifrování hesel v Unixu 246
Jednorázová hesla 250
Metody pro správu konvenčních hesel 255

9: Kontrola integrity 271

Prevence 273
Detekce změn 277
Slovo závěrem 286

10: Auditing a logging 289

Základní logovací soubory 290
Účtování procesů v souborech acct/pacct 299
Logovací soubory jednotlivých příkazů 302
Záznamy práce uživatelů se souborovým systémem 307
Systémový log Unixu (syslog) 309
Swatch: sledování logovacích souborů 318
Ručně vedené záznamy 321
Správa logovacích souborů 324

11: Ochrana proti programovému ohrožení 327

Programové ohrožení - definice 327
Poškození 337

Autoři ... 338
Vstup ... 339
Ochrana ... 340
Ochrana vašeho systému ... 353

12: Fyzická bezpečnost ... 357
Často opomíjená hrozba ... 357
Ochrana počítačového hardwaru ... 359
Ochrana dat ... 374
Příběh: nevydařená inspekce ... 384

13: Personální bezpečnost ... 389
Průzkum minulosti ... 390
V práci ... 391
Lidé z vnějšku ... 395

IV: BEZPEČNOST SÍTĚ A INTERNETU ... 397

14: Telefonní bezpečnost ... 399
Teorie funkce modemů ... 399
Sériová rozhraní ... 401
Sériový protokol RS-232 ... 401
Modemy a bezpečnost ... 405
Modemy a Unix ... 411
Zvýšení bezpečnosti modemů ... 418

15: UUCP ... 421
Popis UUCP ... 422
Verze UUCP ... 426
UUCP a bezpečnost ... 427
Bezpečnost v UUCP Version 2 ... 430
Bezpečnost na BNU UUCP ... 437
Další bezpečnostní úvahy ... 445
Bezpečnostní problémy prvních verzí UUCP ... 446
UUCP na sítích ... 447
Shrnutí ... 448

16: Sítě na bázi TCP/IP 449
Sítě 449
IPv4 - Internet Protocol Version 4 453
Bezpečnost IP 470
Další síťové protokoly 477
Shrnutí 478

17: Služby TCP/IP 479
Základy unixovských internetových serverů 480
Řízení přístupu k serverům 484
Primární unixové síťové služby 485
Bezpečnostní dopady síťových služeb 530
Sledování sítě programem netstat 531
Hlídání sítě 534
Shrnutí 535

18: Bezpečnost WWW 537
Bezpečnost a World Wide Web 537
Provoz bezpečného serveru 539
Řízení přístupu k souborům na serveru 549
Vyloučení možnosti odposlechu 555
Rizika na straně prohlížeče 560
Závislost na třetích stranách 563
Shrnutí 564

19: RPC, NIS, NIS+ a Kerberos 565
Zabezpečení síťových služeb 566
Remote Procedure Call (RPC) 567
Secure RPC (AUTH_DES) 570
Network Information Service (NIS) 579
NIS+ 587
Kerberos 594
Ostatní síťové autentifikační služby 603

20: NFS 605
Úvod do NFS 605
NFS bezpečnost na straně serveru 616
Bezpečnost na straně NFS klienta 621
Závěrem 631

V: POKROČILÁ TÉMATA 635

21: Firewally 637
Co je to firewall? 638
Vytvoření vlastního firewallu 648
Příklad: Cisco router jako propust 652
Nastavení brány 658
Další doporučení 664
Závěrečné poznámky 465

22: Wrappery a proxy 669
Proč wrappery? 669
Wrapper programu sendmail (smap/smapd) 670
tcpwrapper 674
SOCKS 687
UDP Relayer 697
Tvorba vlastních wrapperů 697

23: Tvorba bezpečných SUID a síťových programů 701
Jedna chyba vám může zkazit celý den 701
Tipy pro omezení bezpečnostních chyb 705
Tipy při tvorbě síťových programů 713
Tipy pro tvorbu SUID/SGID programů 716
Tipy pro práci s hesly 719
Tipy pro práci s generátory náhodných čísel 720

VI: POSTUP PŘI NAPADENÍ 729

24: Odhalení průniku 731
Úvod 731
Odhalení útočníka 733
Logovací soubory - odhalení stop po útočníkovi 745
Úklid po útočníkovi 746
Příklad 752
Fáze obnovení 754
Ošetření škod 755

25: Útok zablokováním služeb a možná ochrana .. 757
Destruktivní útoky 758
Útoky přetížením 759
Síťové útoky zablokováním služeb 773

26: Počítačová bezpečnost a legislativa USA 777
Zákonné možnosti po průniku 777
Trestní stíhání 778
Občanské spory 787
Další zodpovědnost 788

27: Komu můžete věřit? 797
Můžete věřit počítači? 797
Můžete věřit dodávce? 801
Můžete věřit lidem? 808
Co z toho všeho plyne 812

VII: PŘÍLOHY 813

A: Bezpečnostní kuchařka 815

B: Důležité soubory 837
Soubory a zařízení související s bezpečností 837
Důležité soubory v domovských adresářích 844
SUID a SGID soubory 844

C: Procesy v Unixu *855*
O procesech 855
Vytváření procesů 864
Signály 865
Příkaz kill 867
Spuštění Unixu a přihlášení se 869

D: Tištěné informace *873*
Bezpečnost Unixu 873
Další počítačová literatura 874
Bezpečnostní periodika 885

E: Elektronické prameny *889*
Mailing listy 890
Usenetové skupiny 894
Stránky WWW 895
Software 896

F: Organizace *905*
Profesní organizace 905
Americké vládní instituce 909
Organizace první pomoci 910

G: Tabulka IP služeb *921*

Rejstřík *X933X*