

Obsah

Obsah	5
Předmluva	9
Úvod	10
Používané konvence	10
1. Systematická bezpečnost.....	12
1.1 Postoj k otázkám bezpečnosti IS.....	12
Podpora managementu	12
Argumenty pro management.....	12
Správci informačního systému	14
Uživatelé IS	14
Cíle zajištění bezpečnosti IS	15
1.2 Bezpečnostní politika.....	15
1.3 Analýza rizik.....	16
Aktiva.....	17
Zranitelná místa.....	17
Hrozby	19
Analýza rizik	19
Ekonomický význam protiopatření	21
1.4 Bezpečnostní audit.....	22
1.5 Kritéria hodnocení zabezpečených informačních systémů	24
Oranžová kniha (Orange book)	24
2. Kryptografie a normy v informačních systémech	28
2.1 Šifrování	28
Symetrické šifrovací algoritmy.....	28
Asymetrické šifrovací algoritmy.....	30
2.2 Ostatní kryptografické technologie	32
DSS – Digital Signature Standard	32
HASH Funkce.....	32
Digitální podpis	33
Proces generování šifrovacích klíčů.....	35
Omezení ITAR.....	35
2.3 Certifikáty a certifikační autority	36
Certifikát	36
Certifikační autorita	36
Použití certifikátů	38
Odvolávání certifikátů.....	38
Formáty certifikátů.....	39
2.4 Systémy pro obnovení šifrovacích klíčů.....	39

3. Zabezpečení lokálních sítí	40
3.1 Kontrola přístupu	40
Jednoduchost a snadná dostupnost hesla	40
Slovníkový útok	41
Nedodržení důvěrnosti hesla	41
Krátkodobé opuštění počítače	42
Stabilní hesla	43
Mnoho hesel	43
Možnost zachycení hesla	44
Hardwarové autentizační prostředky	44
Biometrické systémy	45
3.2 Šifrování dat v lokální síti	46
On-line šifrování souborů	46
Off-line šifrování souborů	47
On-demand šifrování souborů	47
Šifrování výměnných médií	48
Zabezpečení notebooků	49
Bezpečnostní problémy s Windows NT	49
Zabezpečení terminálového přístupu k serverům typu UNIX	50
3.3 Počítačové viry	51
Projevy počítačových virů	52
Technologie pro odhalování virů	53
Antivirové programy	56
Antivirová kontrola a šifrování	59
Koncepce řešení virové problematiky	60
3.4 Auditní záznamy	61
Účel a obsah auditních záznamů	61
Kontrola auditních záznamů	61
Význam AuditLOGů pro uživatele	62
Skartace dat	63
3.5 Zálohování a archivace	65
Zálohování dat	65
Zálohování hardwaru	68
Zálohování zdrojů napájení	69
4. Zabezpečení komunikací	70
4.1 Odposlouchávání sítě	70
4.2 Sítě a komunikace v sítích	73
Jak to chodí v sítích (model ISO/OSI a TCP/IP)	73
Síťové protokoly a bezpečnost	74
4.3 Virtuální privátní síť	75
Propojení lokálních sítí	75
Připojení jednotlivých počítačů k VPN	76
Protokol IPSec	77
VPN a firewall	77

4.4 Šifrování elektronické pošty	77
Plug-in moduly.....	78
Šifrování pošty pomocí PGP.....	78
Public Key Infrastructure (PKI).....	80
Šifrování pošty pomocí IronWare® MailProtect.....	81
4.5 Šifrování FTP protokolu	81
4.6 Šifrování HTTP protokolu	82
4.7 Zabezpečení komunikací prostřednictvím SSL	82
Princip SSL.....	82
Využití SSL v praxi.....	83
4.8 Zabezpečení komunikací prostřednictvím SSH	83
4.9 Vzdálený přístup (remote access)	84
4.10 Firewall	84
Paketový filtr.....	85
Aplikační brána.....	86
Zaznamenávání běhových informací.....	87
Autentizace uživatelů.....	88
Virtuální privátní síť a firewally.....	88
4.11 Testování zranitelnosti sítí	88
Použitá a doporučená literatura	89
Rejstřík	90