

Segurança de Redes em Ambientes Cooperativos

**Emilio Tissato Nakamura
Paulo Lício de Geus**

SUMÁRIO

Agradecimentos	11
Palavra dos autores	13
Sobre os autores	14
Sobre este livro	15
Apresentação	16
Prefácio	18
Parte I ■ Conceitos básicos de segurança	23
Capítulo 1 ■ Introdução	25
Estrutura básica.....	29
Parte I – Conceitos básicos de segurança.....	30
Parte II – Técnicas e tecnologias disponíveis para defesa	31
Parte III – Modelo de segurança para um ambiente cooperativo	33
Capítulo 2 ■ O ambiente cooperativo	35
2.1 A informática como parte dos negócios.....	35
2.2 Ambientes cooperativos.....	38
2.3 Problemas nos ambientes cooperativos.....	39
2.4 Segurança em ambientes cooperativos.....	41
2.5 Conclusão	43
Capítulo 3 ■ A necessidade de segurança	44
3.1 A segurança de redes.....	44
3.2 Maior evolução, maior preocupação com a segurança	48
3.3 Segurança como parte dos negócios	50
3.4 Como a segurança é vista hoje	52
3.5 Investimentos em segurança	54
3.6 Mitos sobre segurança.....	58
3.7 Riscos e considerações quanto à segurança	59
3.8 Segurança <i>versus</i> funcionalidades	61
3.9 Segurança <i>versus</i> produtividade	62
3.10 Uma rede totalmente segura.....	63
3.11 Conclusão.....	64

Capítulo 4 ■ Os riscos que rondam as organizações.....	66
4.1 Os potenciais atacantes.....	66
4.2 Terminologias do mundo dos <i>hackers</i>	78
4.3 Os pontos explorados.....	80
4.4 O planejamento de um ataque.....	83
4.5 Ataques para a obtenção de informações.....	84
4.6 Ataques de negação de serviços.....	103
4.7 Ataque ativo contra o TCP.....	109
4.8 Ataques coordenados.....	116
4.9 Ataques no nível da aplicação.....	121
4.10 Conclusão.....	135
Capítulo 5 ■ Novas funcionalidades e riscos: redes sem fio.....	136
5.1 Evolução e mudanças.....	136
5.2 Características de redes sem fio.....	139
5.3 Segurança em redes sem fio.....	140
5.4 Bluetooth.....	142
5.5 WLAN.....	161
5.6 Conclusão.....	185
Parte II ■ Técnicas e tecnologias disponíveis para defesa.....	187
Capítulo 6 ■ Política de segurança.....	188
6.1 A importância.....	188
6.2 O planejamento.....	189
6.3 Os elementos.....	191
6.4 Considerações sobre a segurança.....	194
6.5 Os pontos a serem tratados.....	196
6.6 A implementação.....	198
6.7 Os maiores obstáculos para a implementação.....	200
6.8 Política para as senhas.....	204
6.9 Política para firewall.....	208
6.10 Política para acesso remoto.....	210
6.11 Política de segurança em ambientes cooperativos.....	211
6.12 Estrutura de uma política de segurança.....	215
6.13 Conclusão.....	219
Capítulo 7 ■ Firewall.....	220
7.1 Definição e função.....	220
7.2 Funcionalidades.....	223
7.3 A evolução técnica.....	226
7.4 As arquiteturas.....	245
7.5 O desempenho.....	251
7.6 O mercado.....	253
7.7 A avaliação do firewall.....	254

7.8 Teste do firewall.....	256
7.9 Problemas relacionados	258
7.10 O firewall não é a solução total de segurança	260
7.11 Conclusão	263
Capítulo 8 ■ Sistema de detecção de intrusão	264
8.1 Objetivos	264
8.2 Características	266
8.3 Tipos	269
8.4 Metodologias de detecção	281
8.5 Inserção e evasão de IDS	288
8.6 Intrusion Prevention System (IPS)	292
8.7 Configuração do IDS.....	294
8.8 Padrões	295
8.9 Localização do IDS na rede	296
8.10 Desempenho	297
8.11 Forense computacional.....	298
8.12 Conclusão	300
Capítulo 9 ■ A criptografia e a PKI.....	301
9.1 O papel da criptografia	301
9.2 A segurança dos sistemas criptográficos	307
9.3 As maiores falhas nos sistemas criptográficos.....	312
9.4 Os ataques aos sistemas criptográficos	313
9.5 Certificados digitais	317
9.6 Infra-estrutura de chave pública.....	318
9.7 Conclusão.....	330
Capítulo 10 ■ Redes privadas virtuais	331
10.1 Motivação e objetivos.....	331
10.2 Implicações	333
10.3 Os fundamentos da VPN	334
10.4 O tunelamento	334
10.5 As configurações.....	335
10.6 Os protocolos de tunelamento	350
10.7 Gerenciamento e controle de tráfego	359
10.8 Desafios	360
10.9 Conclusão	362
Capítulo 11 ■ Autenticação	363
11.1 A identificação e a autorização	363
11.2 Controle de acesso	374
11.3 Single Sign-On (SSO)	376
11.4 Conclusão	380

Parte III ■ Modelo de segurança para um ambiente cooperativo	381
Capítulo 12 ■ As configurações de um ambiente cooperativo	382
12.1 Os cenários até o ambiente cooperativo	382
12.2 Configuração VPN/firewall	406
12.3 Conclusão	411
Capítulo 13 ■ Modelo de segurança para ambientes cooperativos	412
13.1 Os aspectos envolvidos no ambiente cooperativo	412
13.2 As regras de filtragem.....	415
13.3 Manipulação da complexidade das regras de filtragem	427
13.4 Integrando tecnologias – firewall cooperativo.....	432
13.5 Níveis hierárquicos de defesa	435
13.6 Modelo de teias	442
13.7 Conclusão	456
Capítulo 14 ■ Conclusão	458
Referências bibliográficas.....	461
Índice remissivo	477