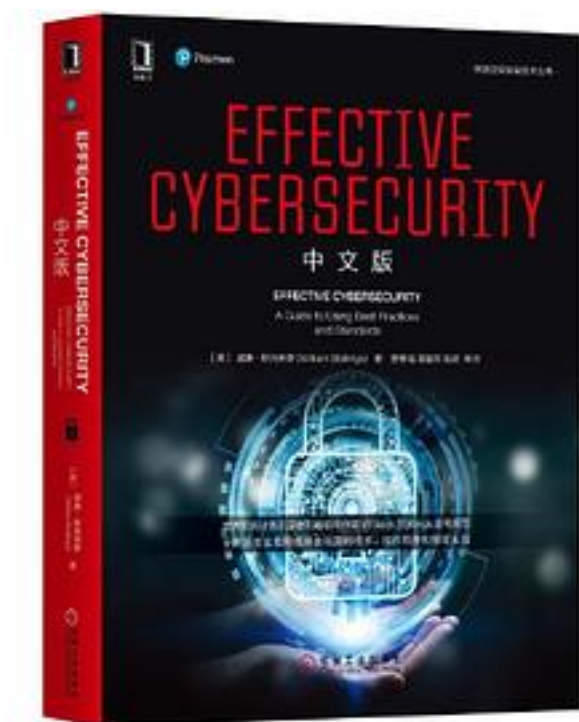


Effective Cybersecurity 中文版



[Effective Cybersecurity 中文版 下载链接1](#)

著者:[美]威廉·斯托林斯 (William Stallings)

出版者:机械工业出版社

出版时间:2020-1

装帧:平装-胶订

isbn:9787111643456

本书是一部在组织中实现网络安全的指导性著作，对于组织的网络安全规划、网络安全功能的管理和网络安全的评估具有重要的指导意义。

全书主要包含三个部分。

第一部分

网络安全规划：介绍管理和控制网络安全功能的方法、定义给定IT环境的特定需求、制定管理安全职能的政策和程序。

第二部分

管理网络安全功能：详细探讨旨在满足定义的安全需求的安全控制。其中第13章涵盖实现有效网络安全的广泛的管理、运营和技术手段。

第三部分 安全评估：总结对网络安全进行评测与改进的相关问题。

作者介绍:

威廉·斯托林斯 (William Stallings) 拥有麻省理工学院计算机科学博士学位和圣母大学电气工程学士学位。在普及计算机安全、计算机网络和计算机体系结构的技术方面做出了独特的贡献。他已经撰写、出版了70多本有关安全、网络和体系结构方面的书籍，有很多作品出现在ACM和IEEE的系列出版物中，并曾13次获得教材和学术专著作者协会颁发的“年度最佳计算机科学教材”奖。目前，他是一名独立技术顾问，其客户包括领先的技术提供者和政府研究机构等。

目录: 译者序

前言

- 第1章 最佳实践、标准与行动计划 1
 - 1.1 网络空间和网络安全的定义 2
 - 1.2 标准和最佳实践文档的价值 4
 - 1.3 信息安全最佳实践标准 5
 - 1.4 ISO/IEC 27000信息安全标准套件 8
 - 1.4.1 ISO 27001 10
 - 1.4.2 ISO 27002 11
 - 1.5 ISO 27000系列与ISF SGP的对应关系 12
 - 1.6 NIST网络安全框架和安全文档 14
 - 1.6.1 NIST网络安全框架 14
 - 1.6.2 NIST安全文档 17
 - 1.7 有效网络防御的CIS关键安全控制 18
 - 1.8 信息安全的COBIT-5 19
 - 1.9 支付卡行业数据安全标准 20
 - 1.10 ITU-T安全文档 21
 - 1.11 有效地实现网络安全 23
 - 1.11.1 网络安全管理流程 24
 - 1.11.2 使用最佳实践和标准文档 25
 - 1.12 关键术语和复习题 26
 - 1.13 参考文献 26
- 第一部分 网络安全规划
- 第2章 安全治理 30
 - 2.1 安全治理和安全管理 31
 - 2.2 安全治理原则和期望结果 32
 - 2.2.1 原则 32
 - 2.2.2 期望结果 33
 - 2.3 安全治理组件 34
 - 2.3.1 战略规划 34
 - 2.3.2 组织结构 36
 - 2.3.3 角色和职责 39
 - 2.3.4 与企业架构集成 41
 - 2.3.5 政策和指导 45
 - 2.4 安全治理方法 45
 - 2.4.1 安全治理框架 45

2.4.2 安全指导	46
2.4.3 责任人、问责人、咨询人和知情人 (RACI) 图表	47
2.5 安全治理评估	48
2.6 安全治理最佳实践	50
2.7 关键术语和复习题	50
2.8 参考文献	51
第3章 信息风险评估	53
3.1 风险评估的概念	54
3.1.1 风险评估面临的挑战	56
3.1.2 风险管理	57
3.1.3 本章结构	59
3.2 资产识别	60
3.2.1 硬件资产	60
3.2.2 软件资产	60
3.2.3 信息资产	60
3.2.4 业务资产	62
3.2.5 资产登记	62
3.3 威胁识别	63
3.3.1 STRIDE威胁模型	63
3.3.2 威胁类型	63
3.3.3 信息来源	65
3.4 控制识别	69
3.5 漏洞识别	72
3.5.1 漏洞类别	73
3.5.2 美国国家漏洞数据库和通用漏洞评分系统	73
3.6 风险评估方法	76
3.6.1 风险的定量评估和定性评估	76
3.6.2 简单的风险分析工作表	80
3.6.3 信息风险因素分析	81
3.7 可能性评估	83
3.7.1 估算威胁事件频率	84
3.7.2 脆弱性估计	84
3.7.3 损害事件频率	86
3.8 影响评估	86
3.8.1 估算主要损害	87
3.8.2 估算次要损害	88
3.8.3 业务影响参考表	89
3.9 风险确定	90
3.10 风险测评	90
3.11 风险处置	91
3.11.1 降低风险	92
3.11.2 维持风险	92
3.11.3 避免风险	92
3.11.4 转移风险	92
3.12 风险评估最佳实践	92
3.13 关键术语和复习题	93
3.14 参考文献	95
第4章 安全管理	96
4.1 安全管理功能	96
4.1.1 安全规划	99
4.1.2 资本规划	101
4.2 安全政策	102
4.2.1 安全政策类别	103
4.2.2 安全政策文档内容	104

4.2.3 安全政策管理指南	106
4.2.4 监控政策	107
4.3 可接受的使用政策	107
4.4 安全管理最佳实践	108
4.5 关键术语和复习题	109
4.6 参考文献	110
第二部分 管理网络安全功能	
第5章 人员管理	112
5.1 人力资源安全	112
5.1.1 招聘流程中的安全性	113
5.1.2 雇佣期间	116
5.1.3 雇佣关系终止	116
5.2 安全意识和教育	117
5.2.1 安全意识	118
5.2.2 网络安全基本程序	122
5.2.3 基于角色的培训	123
5.2.4 教育和认证	123
5.3 人员管理最佳实践	124
5.4 关键术语和复习题	124
5.5 参考文献	125
第6章 信息管理	126
6.1 信息分类和处理	126
6.1.1 信息分类	127
6.1.2 信息标注	130
6.1.3 信息处理	131
6.2 隐私	132
6.2.1 隐私威胁	133
6.2.2 隐私原则和政策	135
6.2.3 隐私控制	138
6.3 文档和记录管理	139
6.3.1 文档管理	140
6.3.2 记录管理	141
6.4 敏感物理信息	142
6.5 信息管理最佳实践	143
6.6 关键术语和复习题	144
6.7 参考文献	145
第7章 物理资产管理	146
7.1 硬件生命周期管理	146
7.1.1 规划	148
7.1.2 采购	148
7.1.3 部署	149
7.1.4 管理	149
7.1.5 处置	149
7.2 办公设备	150
7.2.1 威胁和脆弱性	150
7.2.2 安全控制	152
7.2.3 设备处置	154
7.3 工业控制系统	155
7.3.1 IT系统与工业控制系统的区别	156
7.3.2 ICS安全	157
7.4 移动设备安全	161
7.4.1 移动设备技术	162
7.4.2 移动生态系统	163
7.4.3 漏洞	164

7.4.4 移动设备安全策略	165
7.4.5 移动设备安全资源	169
7.5 物理资产管理最佳实践	170
7.6 关键术语和复习题	171
7.7 参考文献	172
第8章 系统开发	173
8.1 系统开发生命周期	173
8.1.1 NIST SDLC模型	173
8.1.2 SGP的SDLC模型	176
8.1.3 DevOps	177
8.2 将安全性纳入SDLC	181
8.2.1 启动阶段	182
8.2.2 开发/采购阶段	185
8.2.3 实现/评估阶段	187
8.2.4 运行/维护阶段	190
8.2.5 废弃阶段	191
8.3 系统开发管理	192
8.3.1 系统开发方法	193
8.3.2 系统开发环境	193
8.3.3 质量保证	195
8.4 系统开发最佳实践	195
8.5 关键术语和复习题	196
8.6 参考文献	197
第9章 业务应用程序管理	198
9.1 应用程序管理的概念	198
9.1.1 应用程序生命周期管理	199
9.1.2 应用程序项目组合管理	200
9.1.3 应用程序性能管理	203
9.2 公司业务应用程序安全	204
9.2.1 业务应用程序登记	204
9.2.2 业务应用程序保护	205
9.2.3 基于浏览器的应用程序保护	206
9.3 终端用户开发的应用程序	210
9.3.1 EUDA的优点	211
9.3.2 EUDA的风险	211
9.3.3 EUDA安全框架	212
9.4 业务应用程序管理最佳实践	214
9.5 关键术语和复习题	215
9.6 参考文献	216
第10章 系统访问	217
10.1 系统访问的概念	217
10.2 用户身份认证	219
10.2.1 电子用户身份认证模型	219
10.2.2 身份认证方式	221
10.2.3 多因素身份认证	222
10.3 基于口令的身份认证	223
10.3.1 口令的弱点	223
10.3.2 哈希口令的使用	225
10.3.3 用户选择口令的口令破解	226
10.3.4 口令文件访问控制	228
10.3.5 口令选择	228
10.4 基于所有权的身份认证	230
10.4.1 存储卡	230
10.4.2 智能卡	231

- 10.4.3 电子身份证 232
- 10.4.4 一次性口令设备 234
- 10.4.5 基于所有权的身份认证的威胁 235
- 10.4.6 基于所有权的身份认证的安全控制 236
- 10.5 生物特征认证 236
 - 10.5.1 生物特征的指标 236
 - 10.5.2 用于生物识别应用的物理特征 237
 - 10.5.3 生物特征认证系统的操作 238
 - 10.5.4 生物识别的准确率 239
 - 10.5.5 生物特征认证的威胁 240
 - 10.5.6 生物特征认证的安全控制 242
- 10.6 用户身份认证的风险评估 243
 - 10.6.1 身份认证保证级别 243
 - 10.6.2 选择一个AAL 244
 - 10.6.3 选择一种认证方式 246
- 10.7 访问控制 248
 - 10.7.1 主体、客体和访问权限 249
 - 10.7.2 访问控制策略 249
 - 10.7.3 自主访问控制 250
 - 10.7.4 基于角色的访问控制 252
 - 10.7.5 基于属性的访问控制 252
 - 10.7.6 访问控制度量指标 257
- 10.8 客户访问 258
 - 10.8.1 客户访问安排 258
 - 10.8.2 客户合同 258
 - 10.8.3 客户关系 259
 - 10.8.4 保护客户数据 259
- 10.9 系统访问最佳实践 259
- 10.10 关键术语和复习题 260
- 10.11 参考文献 261
- 第11章 系统管理 263
 - 11.1 服务器配置 264
 - 11.1.1 服务器面临的威胁 264
 - 11.1.2 服务器的安全需求 265
 - 11.2 虚拟服务器 266
 - 11.2.1 虚拟化方案 266
 - 11.2.2 虚拟化面临的安全问题 270
 - 11.2.3 安全的虚拟化系统 270
 - 11.3 网络存储系统 272
 - 11.4 服务级别协议 273
 - 11.4.1 网络提供商 274
 - 11.4.2 计算机安全事故响应小组 275
 - 11.4.3 云服务提供商 276
 - 11.5 性能和能力管理 277
 - 11.6 备份 277
 - 11.7 变更管理 278
 - 11.8 系统管理最佳实践 281
 - 11.9 关键术语和复习题 281
 - 11.10 参考文献 282
- 第12章 网络与通信 283
 - 12.1 网络管理的概念 283
 - 12.1.1 网络管理功能 284
 - 12.1.2 网络管理系统 287
 - 12.1.3 网络管理体系结构 290

12.2 防火墙	291
12.2.1 防火墙特性	291
12.2.2 防火墙类型	292
12.2.3 下一代防火墙	298
12.2.4 DMZ网络	298
12.2.5 现代IT边界	299
12.3 虚拟专用网络和IPsec	300
12.3.1 虚拟专用网络	300
12.3.2 IPsec	300
12.3.3 基于防火墙的VPN	302
12.4 网络管理的安全注意事项	303
12.4.1 网络设备配置	303
12.4.2 物理网络管理	304
12.4.3 无线接入	307
12.4.4 外部网络连接	308
12.4.5 防火墙	308
12.4.6 远程维护	309
12.5 电子通信	310
12.5.1 Email	310
12.5.2 即时消息	313
12.5.3 基于IP的语音通信网络	315
12.5.4 电话和会议	319
12.6 网络与通信最佳实践	319
12.7 关键术语和复习题	320
12.8 参考文献	321
第13章 供应链管理与云安全	322
13.1 供应链管理的概念	322
13.1.1 供应链	323
13.1.2 供应链管理	324
13.2 供应链风险管理	325
13.2.1 供应链威胁	328
13.2.2 供应链漏洞	330
13.2.3 供应链安全控制	331
13.2.4 SCRM最佳实践	333
13.3 云计算	334
13.3.1 云计算要素	334
13.3.2 云计算参考架构	338
13.4 云安全	339
13.4.1 云计算的安全注意事项	339
13.4.2 云服务用户的威胁	340
13.4.3 风险评估	341
13.4.4 最佳实践	342
13.4.5 云服务协议	343
13.5 供应链最佳实践	343
13.6 关键术语和复习题	344
13.7 参考文献	345
第14章 技术安全管理	346
14.1 安全架构	347
14.2 恶意软件防护行为	349
14.2.1 恶意软件的类型	350
14.2.2 恶意软件威胁的现状	351
14.2.3 恶意软件防护的实际应用	352
14.3 恶意软件防护软件	354
14.3.1 恶意软件防护软件的功能	354

14.3.2 恶意软件防护软件的管理	355
14.4 身份和访问管理	355
14.4.1 IAM结构	356
14.4.2 联合身份管理	357
14.4.3 IAM规划	359
14.4.4 IAM最佳实践	360
14.5 入侵检测	360
14.5.1 基本原则	361
14.5.2 入侵检测方法	361
14.5.3 基于主机的入侵检测技术	362
14.5.4 基于网络的入侵检测系统	363
14.5.5 IDS最佳实践	365
14.6 数据丢失防护	365
14.6.1 数据分类与识别	366
14.6.2 数据状态	366
14.7 数字版权管理	368
14.7.1 DRM结构和组件	368
14.7.2 DRM最佳实践	370
14.8 密码学解决方案	371
14.8.1 密码技术的使用	371
14.8.2 密码算法	372
14.8.3 密码算法和长度的选择	376
14.8.4 实施密码技术的注意事项	377
14.9 密钥管理	378
14.9.1 密钥类型	380
14.9.2 密钥周期	381
14.9.3 密钥生命周期	382
14.10 公钥基础设施	384
14.10.1 公钥证书	384
14.10.2 PKI结构	385
14.10.3 管理问题	387
14.11 技术安全管理最佳实践	388
14.12 关键术语和复习题	389
14.13 参考文献	390
第15章 威胁与事故管理	392
15.1 技术漏洞管理	392
15.1.1 规划漏洞管理	393
15.1.2 发现已知漏洞	394
15.1.3 扫描漏洞	395
15.1.4 记录和报告	396
15.1.5 修复漏洞	396
15.2 安全事件日志	398
15.2.1 安全事件日志的目标	399
15.2.2 潜在的安全日志来源	399
15.2.3 日志需要记录什么	400
15.2.4 保护日志数据	400
15.2.5 日志管理政策	400
15.3 安全事件管理	401
15.3.1 SEM功能	402
15.3.2 SEM最佳实践	403
15.4 威胁情报	404
15.4.1 威胁分类	404
15.4.2 威胁情报的重要性	406
15.4.3 收集威胁情报	408

- 15.4.4 威胁分析 409
- 15.5 网络攻击的防护 409
 - 15.5.1 网络攻击杀伤链 409
 - 15.5.2 保护和应对措施 412
 - 15.5.3 非恶意软件攻击 414
- 15.6 安全事故管理框架 415
 - 15.6.1 事故管理的目标 416
 - 15.6.2 与信息安全管理体的关系 417
 - 15.6.3 事故管理政策 418
 - 15.6.4 角色和责任 418
 - 15.6.5 事故管理信息 419
 - 15.6.6 事故管理工具 419
- 15.7 安全事故管理流程 420
 - 15.7.1 事故响应的准备阶段 421
 - 15.7.2 检测和分析 421
 - 15.7.3 遏制、根除和恢复 422
 - 15.7.4 事故后的行动 423
- 15.8 紧急修复 424
- 15.9 法律调查 425
 - 15.9.1 准备 426
 - 15.9.2 识别 427
 - 15.9.3 收集 427
 - 15.9.4 保留 428
 - 15.9.5 分析 428
 - 15.9.6 报告 429
- 15.10 威胁和事故管理最佳实践 429
- 15.11 关键术语和复习题 430
- 15.12 参考文献 431
- 第16章 本地环境管理 433
 - 16.1 本地环境安全 433
 - 16.1.1 本地环境总则 434
 - 16.1.2 本地安全协调 435
 - 16.2 物理安全 436
 - 16.2.1 物理安全威胁 436
 - 16.2.2 物理安全官 438
 - 16.2.3 深度防御 439
 - 16.2.4 物理安全：预防和缓解措施 440
 - 16.2.5 物理安全控制 443
 - 16.3 本地环境管理最佳实践 446
 - 16.4 关键术语和复习题 446
 - 16.5 参考文献 447
- 第17章 业务连续性 448
 - 17.1 业务连续性的概念 450
 - 17.1.1 威胁 451
 - 17.1.2 运营中的业务连续性 452
 - 17.1.3 业务连续性目标 453
 - 17.1.4 维持业务连续性的基本组件 454
 - 17.2 业务连续性程序 454
 - 17.2.1 治理 454
 - 17.2.2 业务影响分析 455
 - 17.2.3 风险评估 456
 - 17.2.4 业务连续性政策 457
 - 17.3 业务连续性准备 459
 - 17.3.1 意识 459

17.3.2 培训 460
17.3.3 弹性 461
17.3.4 控制选择 462
17.3.5 业务连续性计划 463
17.3.6 演习和测试 467
17.3.7 性能评估 469
17.4 业务连续性运营 471
17.4.1 应急响应 472
17.4.2 危机管理 473
17.4.3 业务恢复/复原 474
17.5 业务连续性最佳实践 475
17.6 关键术语和复习题 476
17.7 参考文献 477
第三部分 安全评估
第18章 安全监控与改进 480
18.1 安全审计 480
18.1.1 安全审计与报警模型 481
18.1.2 审计数据的收集 482
18.1.3 内部和外部审计 485
18.1.4 安全审计控制 485
18.2 安全性能 489
18.2.1 安全性能评估 489
18.2.2 安全指标的来源 490
18.2.3 信息风险报告 496
18.2.4 信息安全合规性监控 497
18.3 安全监控与改进最佳实践 498
18.4 关键术语和复习题 499
18.5 参考文献 499
附录A 参考文献与标准 501
附录B 专业术语 515
首字母缩略词 529
• • • • • ([收起](#))

[Effective Cybersecurity 中文版_下载链接1](#)

标签

网络安全

计算机

挺好的

安全

中文版

业余爱好

2020

评论

英文原版在亚马逊好评如潮，终于出中文版了，五星推荐！

这本书非常翔实，五百多页的真的啃不完啊。

不愧是一本网络安全百科全书啊，可以说是目前市面上讲解网络安全体系最全面的一本书了。

[Effective Cybersecurity 中文版_下载链接1](#)

书评

[Effective Cybersecurity 中文版_下载链接1](#)