Broadview®
www.broadview.com.cn

企业网络整体安全

—— 内幕大剖析

谌 玺 张 洋 著

本书所附DVD光盘包含超长教学视频

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

企业网络整体安全
——攻防技术内幕大剖析

谌玺 张洋 著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书深入地剖析了构成企业网络整体安全的各部分，包括网络安全概述、网络设备的工作原理、设备造成的安全威胁、各种开放式网络协议，以及开放式网络协议所造成的安全威胁、基于网络设计及网络架构的攻击与防御技术、路由协议的工作原理与攻击防御技术、网络设备的加固技术与检测方法、防火墙的配置、病毒与木马的检测与防御、网络集中验证、访问控制与接入端口的安全技术等。在写作风格上，作者由浅入深，论点有据，将不可见的理论变成形象的数据帧，并经过有序的组织，让读者结束对理论的理想型学习方式，让理论更好理解，可阅读性更强。

本书还讲述了现今最流行的与网络安全密切相关的流量分析技术、流量渗透分析与防御技术、在受到网络攻击时服务质量保证技术、网络安全评估技术、网络安全的加固技术等，大篇幅地揭露了防火墙与杀毒软件视而不见的高危险性攻击与入侵方式、演示防御措施等。本书将附赠教学与实验光盘，使读者感受视听相结合的学习方式，更加形象，更易入手。

本书案例丰富，理论性与实用性都较高，并且以“尊重实验事实，符合实验理论”为编著原则。丰富的案例使其理论性与实用性颇高，非常适合于网络安全项目工程人员、各大企事业单位的信息中心管理人员、CCIE 安全类备考人员、各大高校的专本科学生等。

图书在版编目（CIP）数据

企业网络整体安全：攻防技术内幕大剖析/谌玺，张洋著. —北京：电子工业出版社，2011.8
ISBN 978-7-121-13370-1

Ⅰ. ①企… Ⅱ. ①谌… ②张… Ⅲ. ①企业－计算机网络－安全技术 Ⅳ. ①TP393.180.8

中国版本图书馆 CIP 数据核字（2011）第 074975 号

策划编辑：张月萍
责任编辑：付　睿
特约编辑：赵树刚
印　　刷：北京东光印刷厂
装　　订：三河市皇庄路通装订厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1092　1/16　印张：26.5　字数：696 千字
印　　次：2011 年 8 月第 1 次印刷
印　　数：4000 册　　定价：59.00 元（含 DVD 光盘 1 张）

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系电话：（010）68279077；邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

我国的信息安全建设已进入一个新的时代，在这个新的时代里，网络安全建设已经不再单纯地立足于安全产品、安全软件、病毒处理与木马防御，而是面向整体网络结构、网络设计，甚至于针对网络安全产品本身的加固与防御。

“能够被安全产品或杀毒软件检测出来的安全违规事件，将不再是问题。最大的问题是已经发生了，却没有被查出来的问题。”常规的写作是文献参考，成功的写作是将文献参考变为案例演示，伟大的写作是启发读者。“读之所欲！作之必从！”

——笔者

本书的出版目的

- 重点揭露“网络使用的任何技术都可能构成对网络安全的威胁”。
- 分析并取证针对网络协议与网络结构的攻击是很多安全产品防不胜防的关键原因。
- 曝光黑客入侵的新思路与新方法。

本书写作的环境

本书由多名拥有丰富网络安全渗透检测与纵深防御能力的资深专家亲自参与编著，他们都是具备安全类 CCIE 认证以上高级职称的项目负责人。同时由获得理学博士与硕士学位的高校教师在实验室反复地对理论进行实验研究与验证编成此书，以确保书中提出的重要理论与实验结果完全一致。在写作的过程中，秉承“尊重实验事实，符合实验理论”的原则，大量融汇了各大行业的网络安全实践经验。

本书的独一性

- 重点讲解安全产品无法抵御的攻击方式与入侵手段。
- 本书所有的知识点和攻击防御的演示过程都被制作成详细的演示录像，让读者在良好的视听环境下进行学习。成功地将网络安全的深度理论与高端实验相结合。
- 提出了“基于网络结构与网络设计的安全威胁”的新概念，并且为不同企业的网络环境制订具有企业网络特色的安全防御案例。

关于实验小组成员：张洋、蒋小波、欧阳旭、敖理、罗东旭、陈欢、邹忠林、丁怡颖、范煜恩，是你们用 24 小时轮换工作的方式在一个月内完成了所有的实验和数据帧取证与分析工作。

献辞

谨将本书献给我的外祖父陈子荣先生。虽然您已长辞于人世，但是您十多年的抚育与关怀，让我永生难忘。也正是因为您，我才拥有无穷的力量去战胜写作与录制教学视频过程中的困难与疲惫。愿您的灵魂在天堂得到安息，愿上帝与您同在。“玺得今时仗汝教，鲲鹏展翅向天傲，今君不幸倾人世，兑现宏愿为汝报”。

致谢

本书属于那些经历过漫长黑夜，完成写作的技术团队。参与本书编写的人员有谌玺、张洋、罗森尺、欧阳旭、蒋小波、骆东旭、陈欢、丁怡颖、邹忠林、范煜恩、刘伟、唐晓、梁川、敖理、杨光艺，由于你们给予的全力支持，我将用一生的奋斗来守护这永不熄灭的信仰，忘掉在这个过程中有多么艰辛。我们曾在实验室共存着世界上最美好的回忆，这将烙下创业者们最珍贵的足印。给我抱紧希望的兴奋，我亲爱的同事们，“你们是我一生中最伟大的骄傲”。

感谢重庆电子工程职业学院计算机应用系为实验小组提供了实验环境与支持。特别感谢计算机应用系的龚小勇主任，信息安全教研室的武春岭老师，林倩老师，是你们提供了高校与企业合作的平台，才让我有更多的时间参与到写作工作上，完成第一部校企联合的技术产品。

感谢公司的商务总监罗森尺先生，您让我在事业上懂得了大容大爱的信念。愿您永远平安幸福，取得更辉煌的成绩，我将永远支持您！

使用本书的规则

本书中所使用的路由器、交换机、防火墙如果没有特别说明，都是 Cisco 公司的产品。第 2 章至第 10 章的内容是本书的关键价值所在，这些章节的写作思想是首先将一个知识点的基本理论进行描述，然后讲述知识点所面对的安全威胁，演示黑客入侵的完整过程，最后分析防御方式。每个知识点和相关演示实验都提供了完整的教学视频。建议阅读完一个小节后再观看教学视频，这样会很大程度上加强读者的理解能力与动手能力。

使用图标的规则

 表示该小节配备了实验演示的视频教学。

 表示重要知识点。

本书网络环境所使用的图标

教学视频清单

- 演示：理解集线器的工作原理
- 演示：集线器的入侵与防御
- 演示：网桥、二层交换机的工作原理
- 演示：网桥、二层交换机的入侵与防御
- 演示：交换机“端口安全”功能的使用
- 演示：路由器的工作原理
- 演示：路由器的入侵与防御
- 演示：防火墙的工作原理
- 演示：Sniffer 的安装
- 演示：安装微软网络监视器
- 演示：利用协议分析器分析 ARP 的工作原理
- 演示：利用协议分析器分析 TCP/IP 的工作原理
- 演示：利用协议分析器分析 ICMP 的工作原理
- 演示：DHCP 服务器的配置
- 演示：分析和取证 DHCP 的工作原理

- 演示：配置 DNS 服务与工作原理分析
- 演示：利用协议分析器分析主动 FTP 和被动 FTP 的工作原理
- 演示：配置 Telnet 与 SSH 并分析取证工作原理
- 演示：配置 Web 服务器，取证并分析 HTTP 的数据帧
- 演示：针对 ARP 协议的攻击与防御
- 演示：针对 TCP/IP 协议的攻击与防御
- 演示：针对 ICMP 协议的攻击与防御
- 演示：针对 DHCP 服务器的攻击与防御
- 演示：针对 DNS 服务器的攻击与防御
- 演示：针对 FTP 服务器的攻击与防御
- 演示：针对 UDP 协议的攻击与防御
- 演示：取证分析生成树协议（STP）技术的工作原理
- 演示：基于 STP 技术的攻击与防御
- 演示：分析与取证思科邻居发现协议的工作原理
- 演示：基于 CDP 技术的攻击与防御
- 演示：VLAN 的配置与 VLAN 工作原理的分析取证
- 演示：基于 VLAN 的双标记攻击与防御
- 演示：基于 VTP 技术的攻击与防御
- 演示：基于 VLAN 干道 DTP 技术的攻击与防御
- 演示：取证分析动态路由协议 RIP 的工作原理与实现
- 演示：在 Ubuntu 操作系统上安装 ASS
- 演示：基于动态路由协议 RIP 的入侵与防御
- 演示：取证分析思科 HSRP 的工作原理与实现
- 演示：基于思科的 HSRP 的攻击与防御
- 演示：利用 Sniffer 统计与分析流量
- 演示：利用 NetFlow 统计与分析流量
- 演示：利用 NABR 统计与分析流量
- 演示：取证分析 IP 报文的优先级字段
- 演示：IP 报文的标记
- 演示：队列技术的应用（FIFOQ、WFQ、CBWFQ）
- 演示：使用基于类别的队列（CBWFQ）技术控制企业网络的流程工程
- 演示：使用低延迟队列（LLQ）保证企业语音及视频会议流量
- 演示：通过一个实例来计算 CAR 的正常突发（Bc）与最大突发（Be）
- 演示：利用 CAR 缓解 ICMP 攻击
- 演示：利用 NBAR 防止泛滥下载 MP3、大型的视频文件、图片文件
- 演示：将思科检测 P2P 流量的 PDLM 模块加载到路由器
- 演示：针对 P2P 流量控制的解决方案
- 演示：本地用户登录造成的安全验证分散的问题
- 演示：使用活动目录完成集中验证与一次登录、多次访问
- 演示：分析 Kerberos 验证协议的工作原理
- 演示：SysKey 的配置
- 演示：配置 Windows 操作系统的用户与用户组
- 演示：NTFS 权限使用的原则
- 演示：操作系统各种权限结合的复合应用
- 演示：加密文件系统（EFS）的加密、解密、恢复代理
- 演示：夺取 Windows 操作系统文件及文件夹拥有者权限

- 演示：利用 LC5 破解 Windows 用户口令
- 演示：灰鸽子木马的制作、隐藏、传播及查杀
- 演示：微软 RPC 冲击波蠕虫病毒的入侵与防御
- 演示：U 盘与 Auto 病毒的查杀
- 演示：针对 Windows 操作系统的 TCP 洪水攻击与防御
- 演示：针对 Windows 操作系统的 ICMP 洪水攻击与防御
- 演示：利用微软的基准安全分析器（MBSA）对 Windows 操作系统进行安全评估
- 演示：集中部署 Windows 的补丁分发管理服务器（WSUS 3.0）
- 演示：利用性能监视器实时监控 TCP 洪水攻击
- 演示：建立 Windows 的审核项目——审核用户对资源的访问
- 演示：基于 Windows 系统的镜像阵列
- 演示：基于 Windows 系统的 RAID-5 阵列
- 演示：理解各种备份类型与制订一个合理的备份计划
- 演示：制订安全的数据备份
- 演示：制订自动备份计划
- 演示：使用 UPM 备特佳灾备系统完成数据的实时备份
- 演示：使用 SNMP 完成企业网络设备的集中管理
- 演示：集中收集各种网络设备与服务器的日志文件
- 演示：利用 DHCP Snooping 接合 DAI 防御企业级网络中的 ARP 攻击
- 演示：快速控制企业级网络遭遇病毒后的交叉感染
- 演示：基于思科的交换机完成 802.1x 接入控制
- 演示：思科 IOS 防火墙的基本配置
- 演示：思科 PIX 防火墙的基本配置
- 演示：基于思科 IOS 防火墙的入侵检测系统
- 演示：基于思科 PIX 防火墙的入侵检测系统
- 演示：利用 SDM 加固路由器与交换机的安全
- 演示：基于 Ubuntu 的基本操作与软件的编译安装
- 演示：完成本书最基本的 Ubuntu 操作系统入门
- 演示：在 Ubuntu 下安装 disniff
- 演示：SDM 的基本安装

联系方式

技术讨论微博：http://t.163.com/7734601208
技术电子邮箱：IThonour@163.com
技术讨论 QQ 群：161925248

郑重声明

本书揭露企业网络相关入侵与攻击事例的目的是为了让广大企业网络管理员，提高网络安全意识，加强安全防御手段。书中和教学视频中关于那些不能被安全产品测检的入侵及攻击方法绝不是提供给网络上居心叵测的用户，用于非法目的的。读者实验时请正确地选择实验环境。如果非法应用，产生的一切后果，作者及所在公司不负任何法律责任。

著 者

目　录

第 1 章　网络安全概述 1

1.1　什么是网络安全 1
1.2　典型的网络安全违例事件 1
1.3　引发网络安全违例行为（事件）的途径 2
1.4　企业级网络安全的实现指南 3
1.4.1　网络安全意识 3
1.4.2　初期网络建设就应该考虑安全 3
1.4.3　网络安全管理条例 3
1.4.4　网络安全评估 4
1.4.5　安全加固 4
1.4.6　安全联动 4
1.5　网络安全的范围 4
1.5.1　资产安全 4
1.5.2　风险分析 5
1.5.3　数据安全 5
1.5.4　数据存储和恢复安全 5
1.5.5　数据传输安全 6
1.5.6　数据访问权限安全 6
1.5.7　移动存储设备管理 6
1.5.8　网络安全运行应急预案 6
1.5.9　网络架构安全 6
1.5.10　威胁确定 7
1.5.11　策略制订与安全加固 7
1.5.12　安全应急预案 7
1.6　分析：黑客入侵的过程 8
1.6.1　扫描 8
1.6.2　确定攻击或入侵对象 8
1.6.3　检查对象漏洞 9
1.6.4　分析：黑客的入侵攻击 9
1.7　小结 10

第 2 章　网络设备的工作原理与安全威胁 11
2.1　集线器的工作原理与安全威胁 11
2.2　演示：集线器的入侵与防御 13
2.3　网桥、二层交换机的工作原理与安全威胁 13
2.4　演示：网桥、二层交换机的入侵与防御 20
2.5　路由器的工作原理与安全威胁 24
2.6　演示：路由器的入侵与防御 27
2.7　防火墙的工作原理与安全威胁 32
2.8　小结 38
第 3 章　渗透分析开放式网络协议 39
3.1　为什么要分析开放式协议 39
3.1.1　分析开放式协议的难度 40
3.1.2　利用什么工具分析开放式协议 40
3.1.3　理解 Sniffer_pro 的使用 41
3.2　利用协议分析器分析开放式协议 43
3.2.1　利用协议分析器分析 ARP 的工作原理 43
3.2.2　利用协议分析器分析 TCP/IP 的工作原理 47
3.2.3　利用协议分析器分析 ICMP 的工作原理 49
3.2.4　利用协议分析器分析 DHCP 的工作原理 52
3.2.5　利用协议分析器分析 DNS 的工作原理 55
3.2.6　利用协议分析器分析主动 FTP 与被动 FTP 的工作原理 59
3.2.7　利用协议分析器分析 Telnet 和 SSH 的工作原理 64
3.2.8　利用协议分析器分析 HTTP 的工作原理 70
3.3　小结 73
第 4 章　开放式协议的攻击与防御 74
4.1　演示 ARP 攻击与 ARP 攻击的防御 74
4.2　演示 TCP/IP 攻击与防御 78
4.3　演示基于 ICMP 的攻击与防御 82
4.4　演示：DHCP 攻击与防御 86
4.5　演示：DNS 的攻击与防御 91
4.6　演示：FTP 的攻击与防御 95
4.7　演示：UDP 攻击与防御 101
4.8　小结 105
第 5 章　理解基于网络结构的攻击与防御 106
5.1　基于数据链路层的攻击与防御 106

5.1.1 分析与取证：生成树协议（STP）技术的工作原理 107
5.1.2 演示：基于 STP 技术的攻击与防御 113
5.1.3 分析与取证：思科邻居发现协议（CDP）的工作原理 116
5.1.4 演示：基于 CDP 技术的攻击与防御 118
5.1.5 分析与取证：VLAN 的工作原理与通信过程 120
5.1.6 演示：基于 VLAN 的双标记攻击 127
5.2 基于网络层的攻击与防御 131
5.2.1 路由的基本原理与实现 132
5.2.2 演示：RIP 路由协议的工作原理与实现 132
5.2.3 演示：基于动态路由协议 RIP 的入侵与防御 139
5.2.4 思科 HSRP 的工作原理与实现 144
5.2.5 演示：基于思科的 HSRP 攻击与防御 149
5.3 小结 153
第 6 章 网络安全流量检测与 QoS 技术 154
6.1 流量统计与分析 154
6.1.1 利用 Sniffer 统计与分析流量 154
6.1.2 利用 NetFlow 统计与分析流量 158
6.1.3 利用 NBAR 统计与分析流量 164
6.2 QoS 技术入门 169
6.2.1 详解 IP 报文的优先级字段 171
6.2.2 理解 QoS 的策略过程 173
6.2.3 演示：IP 报文的标记 173
6.3 理解 QoS 队列技术 176
6.3.1 理解 FIFOQ、WFQ、CBWFQ 和 LLQ 176
6.3.2 演示：使用基于类别的队列（CBWFQ）技术控制企业网络的流程工程 185
6.3.3 演示：使用低延迟队列（LLQ）保证企业语音及视频会议流量 191
6.3.4 理解限速器 CAR 的工作原理 193
6.3.5 演示：利用 CAR 缓解 ICMP 攻击 195
6.4 企业级网络流量管理的经典案例演示 197
6.4.1 演示：利用 NBAR 技术完成对典型的网络病毒进行审计并过滤 197
6.4.2 演示：利用 NBAR 防止泛滥下载 MP3、大型的视频文件、图片文件 198
6.4.3 演示：针对 P2P 流量控制的解决方案 202
6.5 小结 206
第 7 章 Windows 操作系统的安全加固 207
7.1 理解 Windows 服务器基本的安全特性 208
7.1.1 操作系统的登录验证 208

7.1.2 配置操作系统的 SysKey 213
7.1.3 操作系统的用户与权限 214
7.1.4 操作系统控制资源访问 219
7.1.5 加密文件系统 222
7.1.6 夺取 Windows 操作系统的文件拥有者权限 229
7.1.7 演示：暴力破解 Windows 安全账户管理器 230
7.2 操作系统面对的安全威胁 232
7.2.1 木马与病毒对操作系统造成的威胁 232
7.2.2 演示：灰鸽子木马的制作、隐藏、传播及防御 234
7.2.3 演示：微软 RPC 的冲击波蠕虫病毒的入侵与防御 241
7.2.4 分析 Auto 病毒的传播原理与防御方式 244
7.2.5 针对 Windows 操作系统做 TCP 洪水攻击的防御 248
7.2.6 针对 Windows 操作系统的 ICMP 洪水攻击与防御 250
7.3 针对 Windows 操作系统的加固措施 256
7.3.1 对 Windows 操作系统进行安全评估 256
7.3.2 集中部署 Windows 的补丁分发管理服务器 261
7.3.3 监控 Windows 的运行情况——利用性能监视器实时监控 TCP 洪水攻击 272
7.3.4 建立 Windows 的审核项目——审核用户对资源的访问 278
7.4 小结 284
第 8 章 灾难保护与备份 285
8.1 灾难保护范围 285
8.1.1 理解磁盘阵列 286
8.1.2 理解 Windows 操作系统的动态磁盘 286
8.1.3 理解 Windows 服务器的简单卷 287
8.1.4 理解 Windows 服务器的跨区与带区阵列 287
8.1.5 理解 Windows 服务器的镜像阵列 288
8.1.6 理解 Windows 服务器的 RAID-5 阵列 289
8.1.7 演示：基于 Windows 系统的镜像阵列 290
8.1.8 演示：基于 Windows 系统的 RAID-5 阵列 293
8.2 数据备份 295
8.2.1 灾难保护并不能替代数据备份 296
8.2.2 理解各种数据备份的方式 296
8.2.3 演示：制订安全的数据备份 298
8.2.4 演示：制订自动备份计划 300
8.2.5 数据备份不能替代实时备份 303
8.2.6 演示：使用 UPM 备特佳灾备系统完成数据的实时备份 304
8.3 小结 313

第 9 章　信息安全的集中管理 314
9.1　为企业网络建立统一的时钟系统 315
9.2　分析与取证：网络集中管理必备协议 SNMP 的工作原理 316
9.3　演示：使用 SNMP 协议完成企业网络设备的集中管理 319
9.4　理解在各种不同系统平台上的日志收集 325
9.5　演示：集中收集各种网络设备与服务器的日志文件 329
9.6　演示：对日志信息的解析与日志的过滤 335
9.7　演示：利用 DHCP Snooping 接合 DAI 技术智能防御网络中的 ARP 攻击 338
9.8　演示：快速控制企业级网络遭遇病毒后的交叉感染 342
9.9　演示：基于桌面系统的接入验证与控制 346
9.10　建立信息安全带外管理方案 360
9.11　加固企业网络的安全配置 362
9.11.1　企业级网络安全设备的种类与应用范围 362
9.11.2　配置思科的 IOS 防火墙 371
9.11.3　配置思科的 PIX 防火墙 376
9.11.4　配置思科基于 IOS 与 PIX 的入侵防御系统 383
9.11.5　利用 SDM 加固路由器与交换机的安全 395
9.12　小结 400
附录 A　和本书有关的 Ubuntu 操作系统的使用基础 401
附录 B　P2P 软件常用的端口号 405
附录 C　SDM 的安装使用 407

第 1 章　网络安全概述

本章关键价值：

通过本章的学习，理解网络安全概念、网络安全的范围、引发网络安全违例行为（事件）的途径，了解企业级网络安全的实现指南，熟悉黑客入侵的过程等。

1.1　什么是网络安全

网络安全是指通过各种技术手段和网络管理措施，保障网络系统的硬件、软件及网络系统中的数据的安全，不会因偶然或恶意的破坏、更改、泄露导致系统和网络服务运行不正常。从而确保整个网络上信息的保密性、安全性、可用性、真实性、完整性和可控性。

注意：现代化企业网络的整体安全，已不仅仅是病毒、木马、攻击这样单纯的范畴，还包括网络通信设备（路由器和交换机）、网络安全设备、应用系统、业务软件、网络设计与架构技术等。这些都属于企业网络整体安全。本书也将从上述的每一个内容来分析企业整体网络安全。

1.2　典型的网络安全违例事件

近年来，随着信息网络的飞速发展，网络与人们的关系日趋紧密，如今已经成为人们生活中不可或缺的一部分，它拉近了人与人之间的距离，改变了人们的工作方式，在人们的生产、生活和娱乐中都发挥着重要作用。但是，伴随而来的安全问题也让人不寒而栗。近几年来网络安全违例事件层出不穷，下面看几个著名的网络安全违例事件。

1988 年 11 月 2 日，美国康奈尔大学的学生罗伯特·莫瑞斯，在互联网上放入了第一个“蠕虫”病毒，从而导致了“蠕虫”大规模地泛滥。

1994 年末，俄罗斯黑客弗拉基米尔·利文与其伙伴从圣彼得堡的一家小软件公司的连网计算机上，向美国花旗银行发动了一连串攻击，通过电子转账方式，从花旗银行窃取了 1100 万美元。

1996 年 12 月 29 日，黑客侵入美国空军的全球网网站并将其主页肆意改动，其中有关空军介绍、新闻发布等内容被替换成一段简短的黄色录像，且声称美国政府所说的一切都是谎言。迫使美国国防部一度关闭了其他 80 多个军方网站。

1999 年大卫斯密斯编写了世界上首个具有全球破坏力的病毒——Melissa。Melissa 病毒使世界上 300 多家公司的计算机系统崩溃，造成的损失接近 4 亿美金。

还有我国首例制作计算机病毒案例：2006 年 10 月，武汉人李俊编写了名为“熊猫烧香”的蠕虫变种病毒，之后在网络中广泛传播，造成大面积的网络瘫痪。

1.3 引发网络安全违例行为（事件）的途径

引发网络安全违例事件的途径已经不再是被黑客攻击而导致网络不安全，而是已经涉及各个方面，如员工误操作、色情网站、赌博网站、共享文件夹、下载数据、移动存储介质、电子邮件、QQ 感染等感染途径。其具体的违例实例事件如下。

员工误操作：在某企业中，由于当初在对网络设计规划的阶段，没有充分地考虑到接入网络的用户数量，导致网络接口数量不足。用户为了接入网络，私自接了一个宽带路由器，而该宽带路由器又有 DHCP 功能，并且已经打开。当初企业网络建设的时候已经架设了一台 DHCP 服务器，用于给用户分配 IP 地址。这样当下次网络中有用户要申请 IP 地址的时候，就有可能得到宽带路由器给的 IP 地址而导致用户不能正常地访问网络中的数据。这就导致了一个安全违例的事件。

色情网站：在色情网站上，病毒的感染有很多的途径。当去访问某个正常网站时，可能会被劫持到色情网站上去。当用户被劫持而访问到色情网站时，首先该色情网站通过它在其首页上挂的病毒来感染用户的计算机，或者是该网站提醒用户下载安装什么软件，这时也有可能被感染。

赌博网站：赌博网站是病毒最喜欢感染的网站，因为该类型的网站可以给攻击者提供利益，所以在访问该类网站的时候，是最容易被感染木马的，从而使个人账户信息被盗窃。

共享文件夹：某一个医疗卫生企业，在一段时间内，其医保服务器在没有大量用户连接使用时，网络流量高达 70%～80%，使该医疗服务企业不能正常收费和开医嘱。导致此结果的原因是该企业中需要使用共享打印机和共享文件夹，对于文件共享来说使用的端口是 UDP 的 137、138 端口，以及 TCP 的 139、445 端口，而这几个端口是洪水攻击和蠕虫攻击的常用端口。对于该企业而言，是受到了基于 139 端口的 ARP 洪水攻击，从而使医保服务器的网卡占有率居高不下。

下载数据：不管对于企业还是个人用户来说，下载数据是一个高频率的操作，用户可能是通过一个网络链接去下载或者是通过 FTP 去下载等。当用户是通过一个网络链接去下载时，如果该链接是一个带了病毒的链接，那么用户的计算机很有可能被病毒感染。或者用户下载的软件当中被注入了病毒，当用户去安装该软件时，病毒也同时感染了其计算机。比如，病毒感染了 EXE 安装文件，当用户去点击此安装文件的时候，其计算机就会被感染病毒。

移动存储介质：在某高校，由于学生的计算机是不可控的，使用如 U 盘、移动硬盘等就可以随意地连接到自己的计算机上，这样就导致了许多病毒通过这个存储介质感染到了学生的个人计算机。当该计算机连接到学校的网络的时候，该病毒就利用该计算机作为一个载体

向整个网络发动攻击或者去感染其他的计算机，同时被感染的计算机再次向网络中发动攻击，使其占用大量的网络流量，从而使该校学生上网经常出现断网或者是网络速度很慢的情况。该校最后实施了一个暂避的方法，就是购买了一套杀毒软件，分发给所有的同学。所以，移动存储介质也是病毒感染的一个重要途径。

电子邮件：通过电子邮件的感染情况最常见的是当用户接收一封邮件时，里面可能包含了一些链接或者可供下载的附件，而这些链接可能连接的是一个带有病毒或者木马的程序，这样，用户的计算机就会被病毒感染。还有就是，可供下载的附件，这个附件可能就是一个病毒程序，从而使用户的计算机感染病毒。

QQ 感染：通过 QQ 感染主要是利用了人们的好奇心，对于 QQ 用户，经常会遇到“你的好友给你点了一首歌”、“你的好友给你推荐了一个××网站”之类的消息，并且给了一个链接，当用户去点击这个链接时，可能在弹出来的那个网页上就挂了一些病毒，并且已经感染了用户的计算机。

1.4　企业级网络安全的实现指南

1.4.1　网络安全意识

随着信息网络的飞速发展，它已经涉及各行各业，包括政府、军事、金融，等等。信息网络中不但承载着它们正常的业务流量，而且还拥有各行业的重要数据甚至是国家军事机密。这就难免遭到政治对手、商业敌人的窃取或攻击。另外，网络实体也会遭到外部因素的侵害（如自然灾害、电压、偷盗等）。所以，必须提高网络安全意识。良好的网络安全意识能帮助用户无论是在最初的网络架设还是后期运维中，都将会有一个正确的思维与方向。

1.4.2　初期网络建设就应该考虑安全

企业级安全网络的建设包括网络的设计与架设。有了良好的网络安全意识，对于初期的网络建设而言，“安全”必定成为人们网络架设中考虑的重要因素之一。因为它直接决定了网络的健壮性，后期使用的高可用性、高性能等。

首先，科学合理的网络设计是实现企业级网络安全的第一步。它要综合考虑所有安全因素，例如，网络结构是否合理、安全设备的选择是否合理、安全设备的布置是否科学等。一个成功的网络设计方案必定拥有完美的安全设计部分。有了科学合理的网络设计方案，才能执行第二步的网络架设。当然，网络的架设一定要严格按照前期制订好的设计方案，以确保初期建设的质量和方便后期的运维。

1.4.3　网络安全管理条例

网络建设完成之后，该怎么使用就有学问了。要知道，80%以上的网络安全违例事件都

发生在网络内部。所以，建立一套完善的网络安全条例来规范对网络的使用是必不可少的，以避免或减少安全违例事件的发生。

1.4.4 网络安全评估

对于一个拥有良好网络安全意识的网络管理者而言，科学的企业网络设计和架设，以及健全的网络安全条例的实施，也只是“企业级网络安全实施”的前半部分。

互联网技术在飞速发展，伴随着的病毒和攻击也在不断发展，当网络使用到一定程度之后，问题必将出现。比如说：后期管理体制的松懈导致违例事件；新型病毒的侵入；新型攻击方式。如果企业自己的技术人员对于这些问题无能为力，导致问题搁置、网络瘫痪等，此时该怎么办？那么，这时企业就需要一个资深的网络安全专家团队，来保障企业全方位的网络安全，使其良性运行。

网络安全评估小组会对企业做一个全方位的安全评估，之后会试验并整合评估信息，将其交予企业，让企业实时地了解自己网络的状态、安全指数，等等，做到真正了解自己的网络。

1.4.5 安全加固

前期的安全评估完成之后，网络安全专家团队会针对前期评估信息给出解决方案，对网络进行安全加固。比如，补丁的更新、安全策略实施、新管理条例的制订，等等。

1.4.6 安全联动

通常，企业对违例事件有自己的安全报警、安全防御系统（如 IDS、IPS 等），以及相应的管理机制。但是当发生了安全违例的事件后，只能通过某一个单一的方面查找发生违例事件的原因和单一的处理方法，如 IDS 指出某一台主机正在遭受攻击，而企业网络管理人员往往只针对该主机进行处理，比如，更新补丁、更新杀毒程序，而没有一个全局性检查。网络安全联动性的中心思想就在于“联动”。当安全违例事件发生之后，注意力并不是全部放在事故点上，而是本着联动的思想全方位地取证，科学地试验，找出违例根源，最后对症下药。另外，安全联动性还要在安全防御上发挥作用。利用自己手中的安全资源，将其联动起来，网络才更坚固，即使发生违例事件，也可以多方取证、对照调查，从而减少误报，而非仅靠一台设备、一项数据来判断问题。

1.5 网络安全的范围

1.5.1 资产安全

企业资产包括无形资产和有形资产两个方面。无形资产包括商标权、专利权、专有技术、