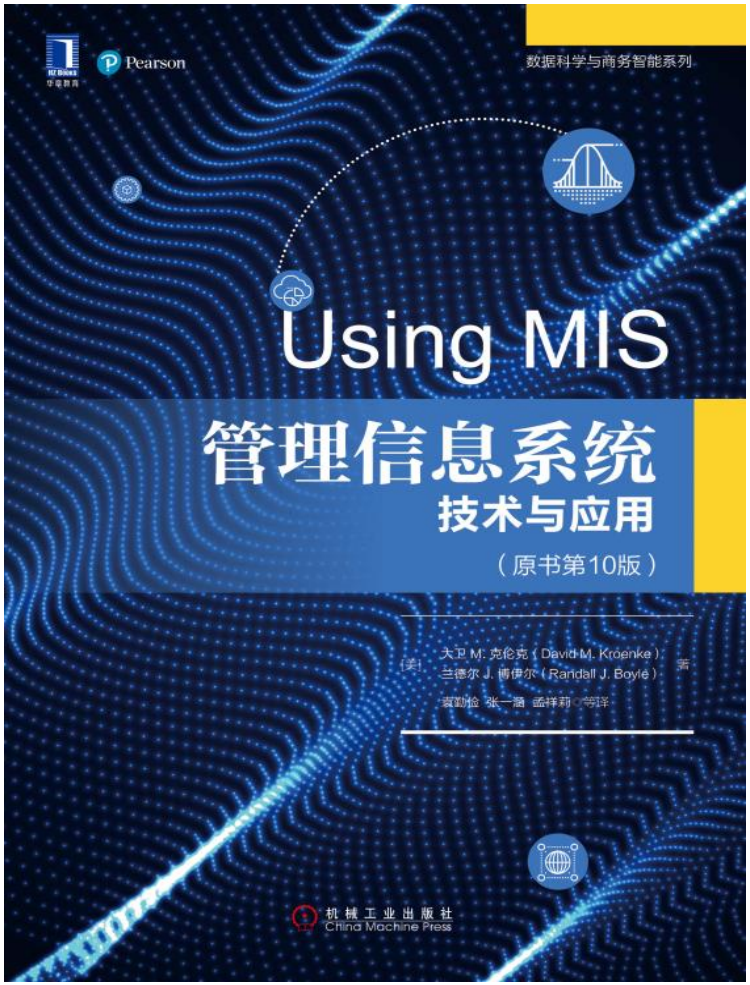
管理信息系统：技术与应用



第10章　信息系统安全

“我想你会了解到我们确实很重视安全问题。”

- 与运动健身设备制造商CanyonBack Fitness（潜在的ARES伙伴）的视频会议。
- 将ARES与CanyonBack运动自行车整合起来存在安全隐患方面的担忧。
- ARES系统是否具有可接受的安全级别？
- 他们的自行车会被黑客袭击吗？客户会受伤吗？个人数据会被盗吗？

“我想你会了解到我们确实很重视安全问题。”（续）

- ARES实施安全编码实践和安全数据备份。
- 用户与单选按钮、下拉框和其他交互式AR元素进行交互。
- 降低了SQL注入攻击的可能性。
- 新技术通常会带来新风险。

章节导览

10-1 信息系统安全的目标是什么
10-2 计算机安全问题有多大
10-3 个人应如何应对安全威胁
10-4 组织应如何应对安全威胁
10-5 技术安全保障如何防范安全威胁
10-6 数据安全保障如何防范安全威胁
10-7 人员安全保障如何防范安全威胁
10-8 组织应如何应对安全事件
10-9 2027？

信息系统安全威胁

10-1 信息系统安全的目标是什么

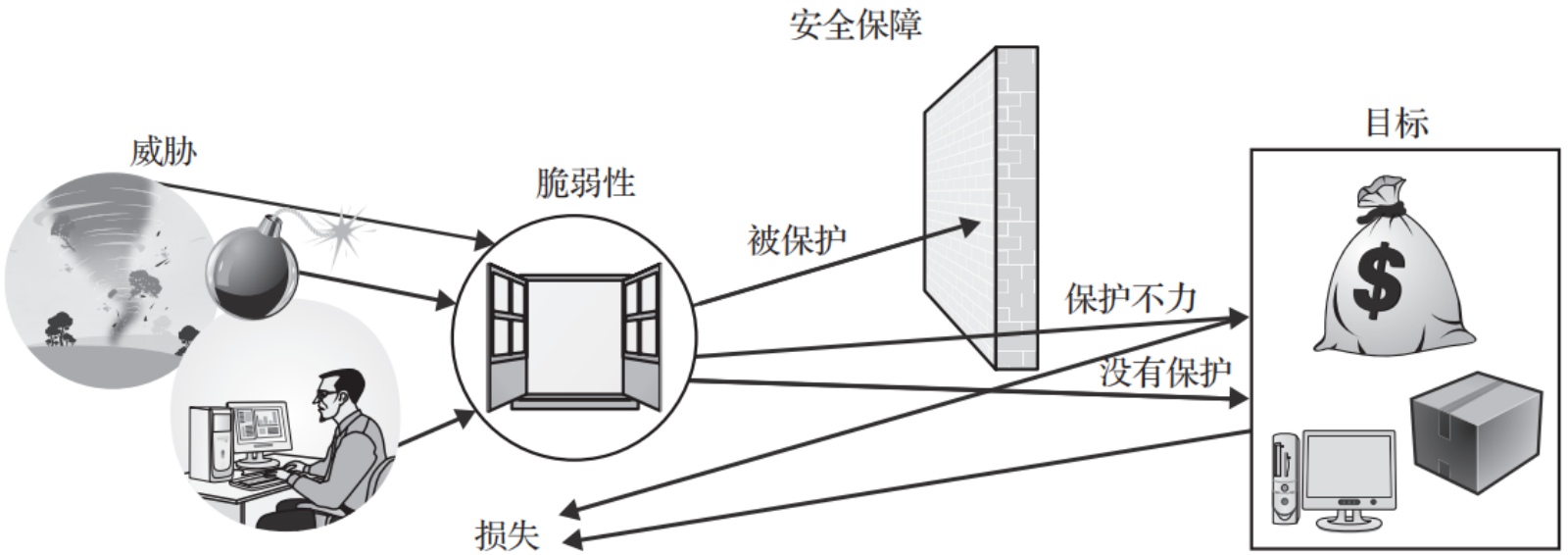


图 10-1　威胁 / 损失情况

威胁 / 损失的举例

10-1 信息系统安全的目标是什么

表 10-1 威胁 / 损失的举例

威胁 / 目标	脆弱性	安全保障	结果	解释
黑客想要盗取你的银行登录凭据	黑客创建一个与你的银行网站几乎相同的钓鱼网站	仅访问使用 https 的网站	没有损失	有效的安全保障
		不采取行动	损失银行登录凭据	无效的安全保障
员工向 Google+ 群组放入敏感数据	公众访问不安全的组	密码 处理规程 员工培训	损失敏感数据	无效的安全保障

威胁的来源是什么？

10-1 信息系统安全的目标是什么

表 10-2 安全问题和来源

		威胁		
		人为失误	计算机犯罪	自然事件和灾害
损失	未经授权的数据泄露	程序错误	假托钓鱼 电子欺骗 嗅探 黑客	恢复期间泄露
	不正确的数据修改	程序错误 不正确的处理规程 无效的计算控制 系统错误	黑客	不正确的数据恢复
	服务错误	程序错误 开发和安装错误	篡夺	不正确的服务恢复
	拒绝服务（DoS）	事故	DoS 攻击	服务中断
	基础设施损失	事故	盗窃 恐怖主义活动	财产损失

存在哪些类型的安全损失？

10-1 信息系统安全的目标是什么

- 未经授权的泄漏
  - 假托
  - 网络钓鱼
  - 欺骗
    - IP欺骗
    - 电子邮件欺骗
  - 嗅探器驱动
    - 战争驾驶者
  - 黑客
  - 自然灾害

不正确的数据修改

- 不正确地遵循处理规程或处理规程设计不正确。
- 增加客户的折扣或错误地修改员工的工资。
- 在公司的网站上放置不正确的数据。
- 原因
  - 系统内部控制不当。
  - 系统误差。
  - 灾难发生后的故障恢复操作。

服务错误

10-1 信息系统安全的目标是什么

- 不正确的数据修改
- 系统运作错误
- 处理规程的错误
- 程序设计错误
- IT安装错误
- 篡位
- 拒绝服务（无意）
- 拒绝服务攻击（有意）

基础设施损失

- 人为事故
- 盗窃和恐怖事件
- 心怀不满、被解雇的员工
- 自然灾害
- 高级持续性威胁
  - APT29 （俄罗斯）和Deep Panda （中国）
  - 从美国公司窃取知识产权。

信息系统安全的目标

10-1 信息系统安全的目标是什么

- 在损失风险和实施安全保障的成本之间找到适当的平衡。
- 保护行动
  - 使用杀毒软件
  - 删除浏览器cookies?
  - 做出适当的权衡来保护你自己和你的事业。

六种类型的计算机犯罪平均成本和总事故百分比

表 10-3 六种类型的计算机犯罪平均成本和总事故百分比（六种最昂贵的类型）

	2010	2011	2012	2013	2014	2015
拒绝服务	NA	187 506 美元（17%）	172 238 美元（20%）	243 913 美元（21%）	166 545 美元（18%）	255 470 美元（16%）
内鬼	100 300 美元（11%）	105 352 美元（9%）	166 251 美元（8%）	198 769 美元（8%）	213 542 美元（8%）	179 805 美元（10%）
基于 Web 的攻击	143 209 美元（15%）	141 647 美元（12%）	125 795 美元（13%）	125 101 美元（12%）	116 424 美元（14%）	125 633 美元（12%）
恶意代码	124 083 美元（26%）	126 787 美元（23%）	109 533 美元（26%）	102 216 美元（21%）	91 500 美元（23%）	164 500 美元（24%）
网络钓鱼与社会工程	35 514 美元（12%）	30 397 美元（9%）	18 040 美元（7%）	21 094 美元（11%）	45 959 美元（13%）	23 470 美元（14%）
设备被盗	25 663 美元（17%）	24 968 美元（13%）	23 541 美元（12%）	20 070 美元（9%）	43 565 美元（10%）	16 588 美元（7%）

资料来源：Data from Ponemon Institute. 2015 Cost of Cyber Crime Study: United States, October 2015, p. 12.

计算机犯罪的严重性

10-2 计算机安全问题有多大

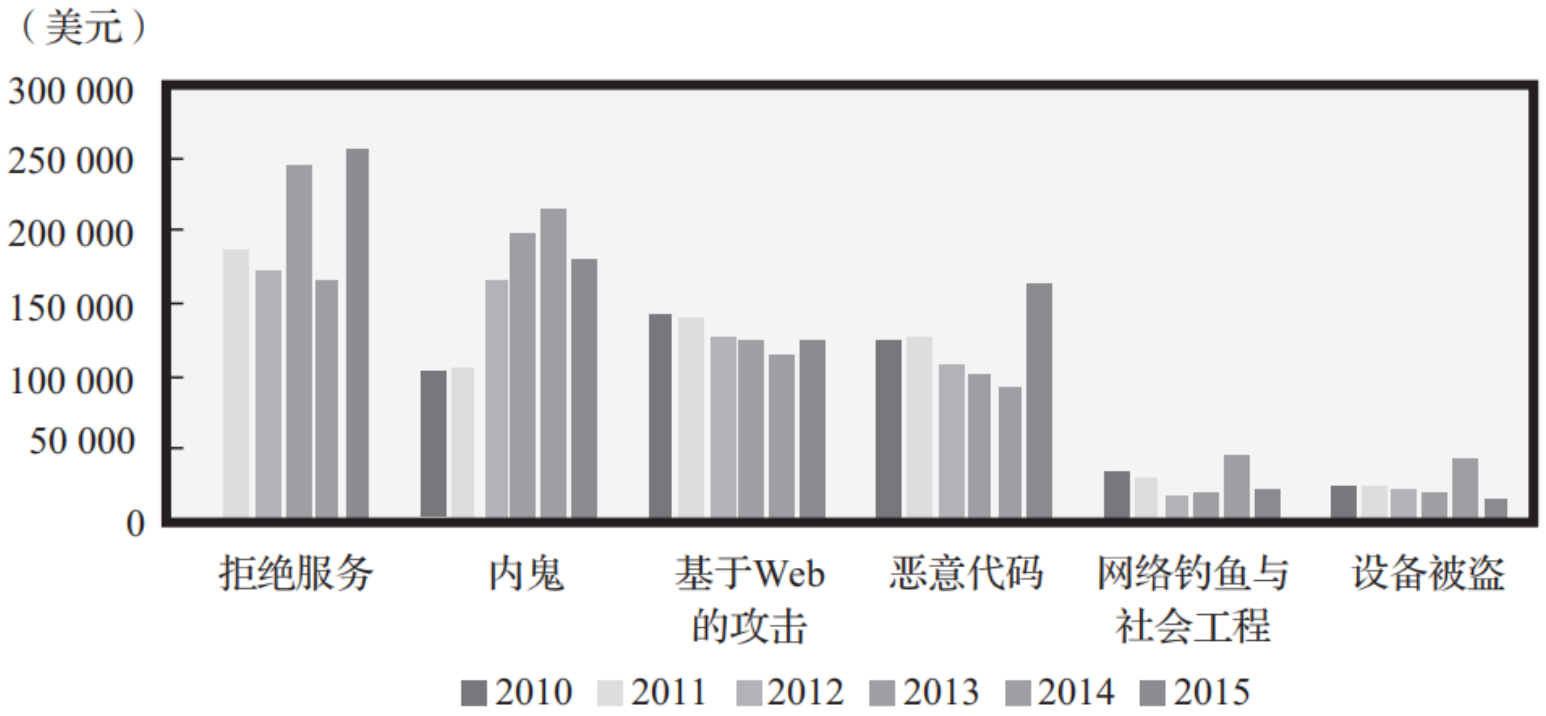


图 10-2　计算机犯罪成本

波尼蒙研究所的研究结果（2015）

- 过去一年中计算机犯罪的增加大多来自恶意代码和拒绝服务攻击。
- 信息损失是成本最高的计算机犯罪。
- 与网络犯罪有关的内部成本一半以上来自检测和恢复。
- 安全保障确实有效。

个人安全保障

10-3 个人应如何应对安全威胁

表 10-4 个人安全保障

• 认真对待安全问题
• 设置高强度密码
• 使用混合密码
• 不使用电子邮件或即时消息发送有价值的数据
• 在可信的、声誉好的供应商那里使用 https 链接
• 转移计算机中的高价值资产
• 删除浏览历史记录、临时文件和 cookie（使用 CCleaner 或其他类似产品）
• 定期更新杀毒软件
• 向你的同事说明安全忧虑
• 遵循组织安全指示和指导原则
• 考虑所有业务活动中的安全性问题

2015黑帽新形式

探秘

- 简要汇报如何进行黑客攻击。
- 展示如何利用硬件、软件、协议或系统的弱点，包括智能手机、物联网设备、汽车等等。
- 鼓励企业修复产品脆弱性。
- 作为黑客、开发商、制造商和政府机构的教育论坛。

2015黑帽新形式（续）

探秘

- 詹妮弗·格兰克（Jennifer Granick）的主题演讲
  - 互联网由于集中化和方便的需求而逐渐减少自由和开发。
  - 一些大公司正在控制大部分互联网行为。
  - 这些公司可以用来审查、监测和控制用户行为。
  - 允许一些技术集中的企业完全控制我们的生活是不明智的。

安全政策

- 高级管理层建立全公司的安全政策：
  - 组织将存储哪些安全数据。
  - 它将如何处理这些数据。
  - 数据是否会与其他组织共享。
  - 员工和其他人如何获取有关他们的数据副本。
  - 员工和其他人如何请求更改不准确的数据。
- 高级管理层管理风险。

五个部分的安全保障

10-4 组织应如何应对安全威胁

图10-3 五个部分的安全保障

隐私保护

伦理指南

- “解决问题的最好办法是不要拥有它。”
  - 拒绝提供敏感数据。
  - 不要收集你不需要的数据。
- 1999年的“格雷姆-里奇-比利雷法”（“GLB Act”）
- 1974年的《隐私法》
- 1996年的《健康保险携带和责任法》(HIPAA)
- 1988年的《澳大利亚隐私法》
  - 不仅管理政府和医疗保健数据，而且管理收入超过300万澳元的企业的记录数据。

隐私保护： Wrap Up

伦理指南

- 商务人士在请求、存储或传播数据时，必须考虑合法性、道德性和常识。
- 仔细考虑你通过公共无线网络打开的电子邮件。
- 使用长且复杂的密码。
- 如果不确定，不要提供数据。

技术安全保障

10-5 技术安全保障如何防范安全威胁

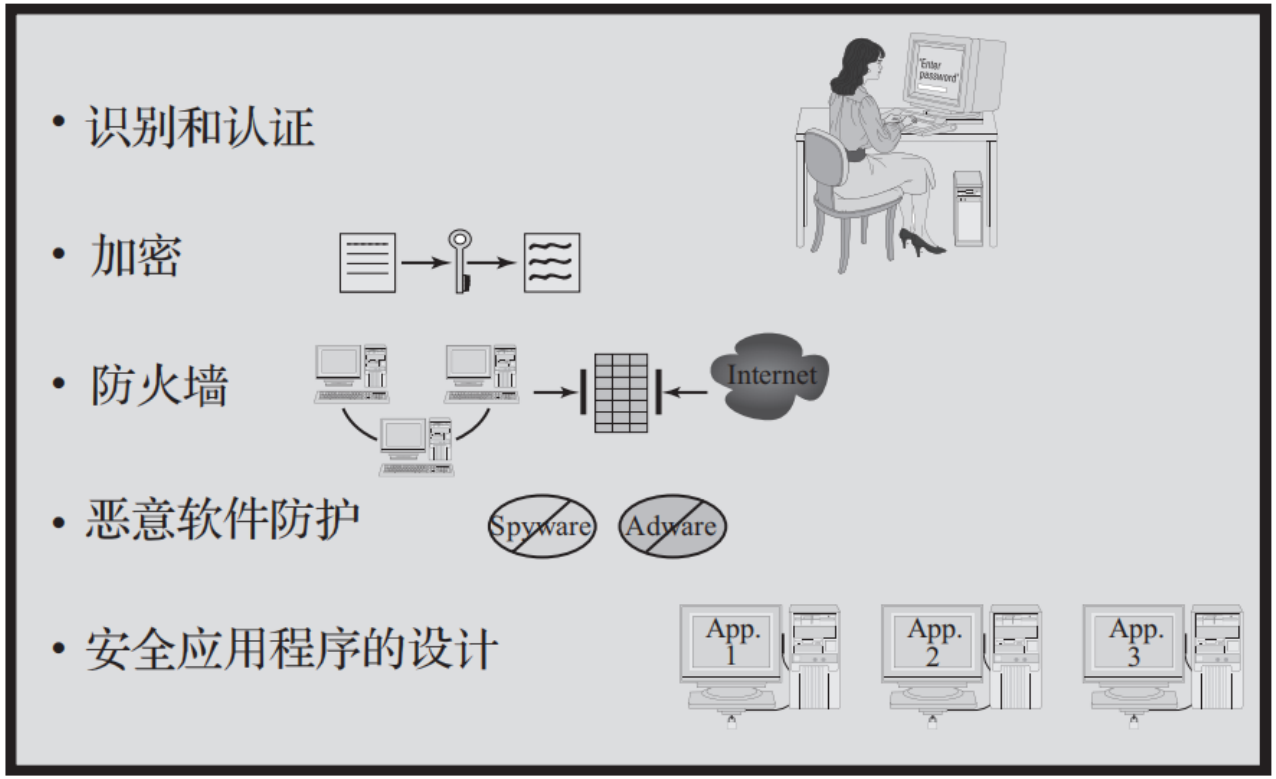


图10-4　技术安全保障

https（SSL 或 TLS）的原理

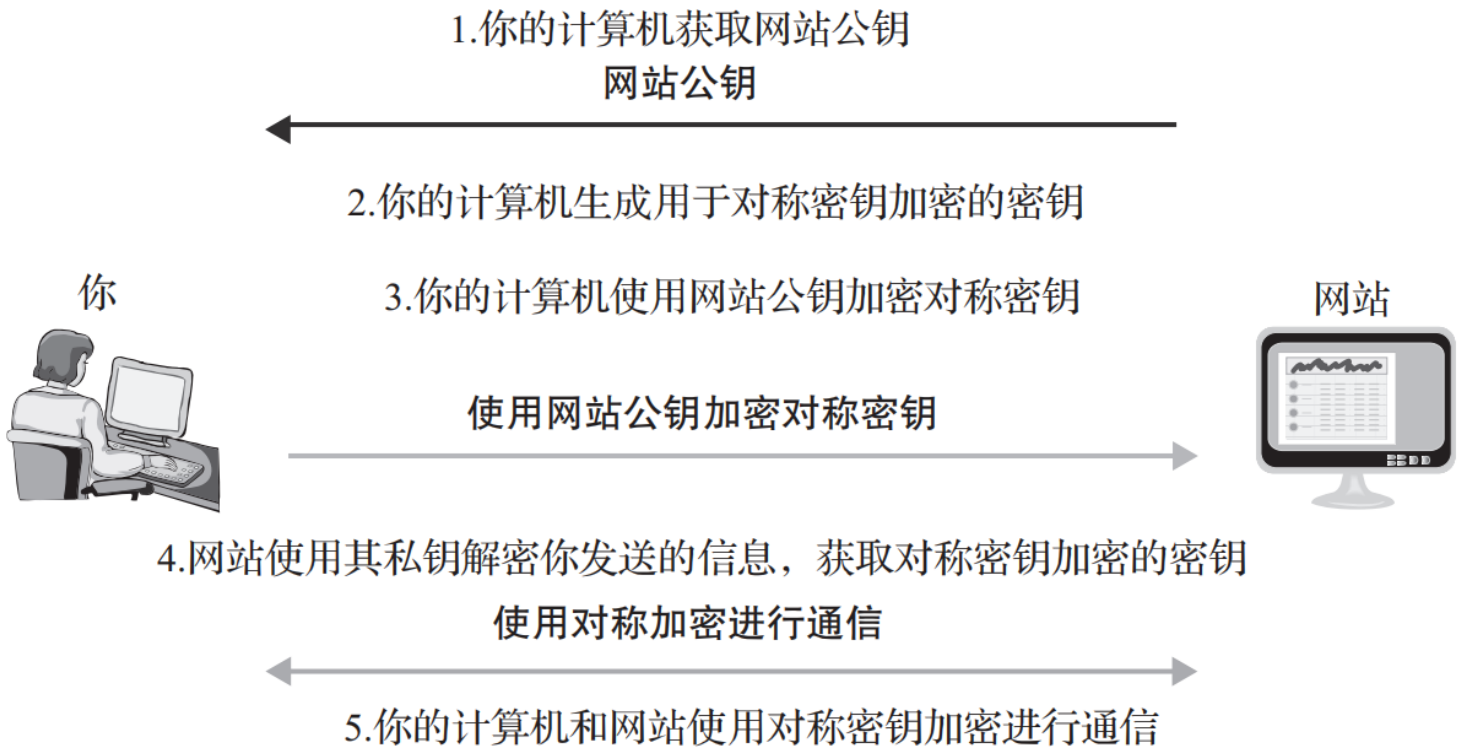


图 10-5 https（SSL 或 TLS）的原理

多个防火墙的使用

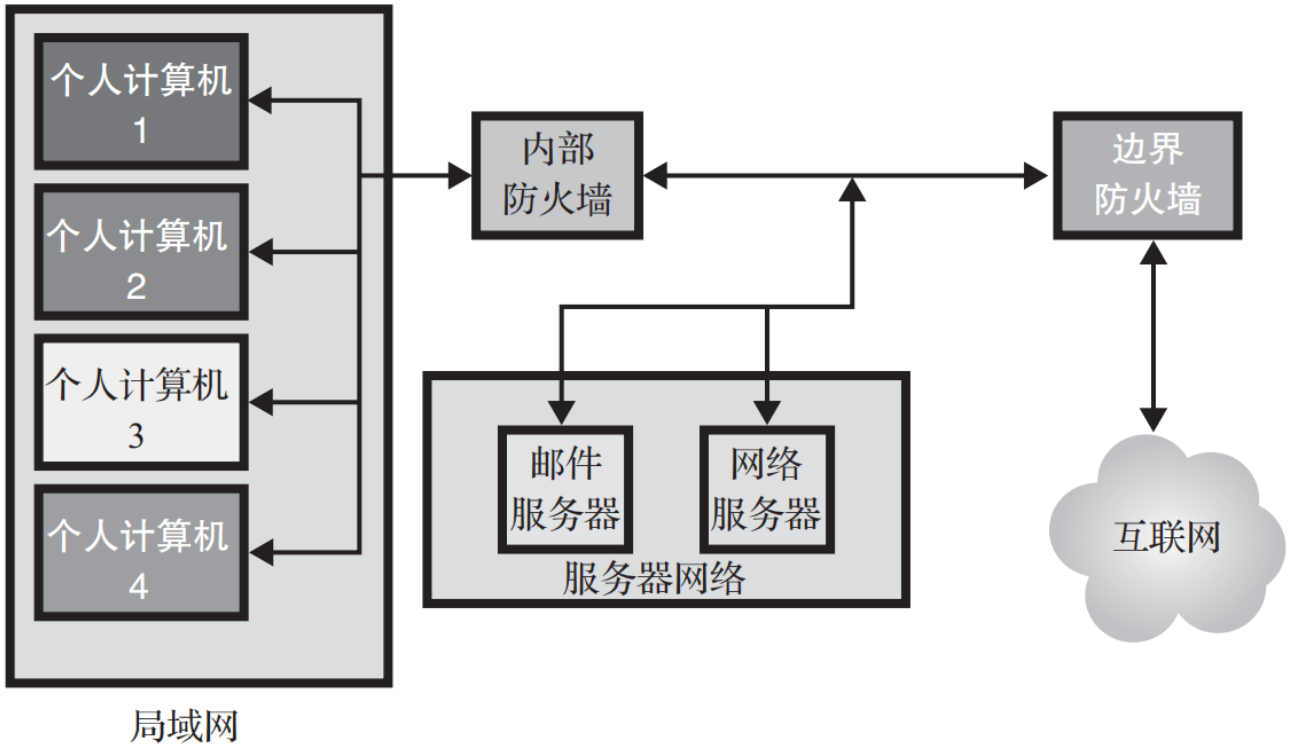


图 10-6　多个防火墙的使用

恶意软件防护（病毒、特洛伊木马、蠕虫）

1. 安装防病毒和反间谍软件程序。
2. 频繁扫描计算机。
3. 更新恶意软件定义。
4. 仅从已知来源打开电子邮件附件。
5. 安装更新后的软件。
6. 只浏览有信誉的网站。

广告软件和间谍软件的症状以及恶意软件的类型

表10–5 广告软件和间谍软件症状

• 系统启动变慢
• 系统反应变慢
• 许多弹出式广告
• 浏览器主页的可疑更改
• 任务栏和其他系统界面的可疑更改
• 异常的硬盘活动

- 恶意软件
  - 病毒
  - 特洛伊木马
  - 蠕虫
  - 间谍软件
  - 广告软件
  - 勒索软件
  - 有效载荷

安全应用程序的设计

- SQL注入攻击
  - 用户将一个SQL语句输入到一个要输入名称或其他数据的表单。
  - 结果
    - SQL代码成为数据库命令的一部分。
    - 可能会产生不当的数据泄露、数据损失和丢失。
  - 精心设计的应用程序将使这种注入无效。

数据安全保障

10-6 数据安全保障如何防范安全威胁

表 10-6 数据安全保障

• 明确数据政策
• 数据权利和责任
• 由密码认证的用户账户执行权限
• 数据加密
• 备份和恢复程序
• 物理安全

- 数据安全保障
- 数据管理
- 密钥托管

内部员工安全政策

10-7 人员安全保障如何防范安全威胁

- 职位定义
  - 分离职责和权限
  - 确定最低权限
  - 文档位置的敏感性
- 招聘和审查

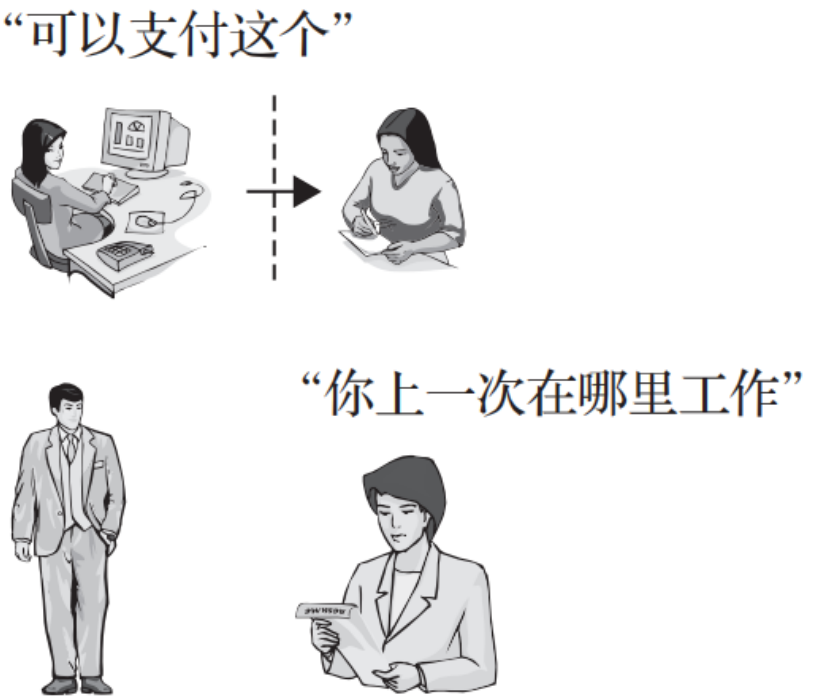


图 10–7 内部员工的安全政策

内部员工安全政策（续）

10-7 人员安全保障如何防范安全威胁

- 宣传和执行
  - 责任
  - 问责
  - 合规
- 离职
  - 友好
  - 不友好

图 10–7 内部员工的安全政策

非员工人员安全保障

10-7 人员安全保障如何防范安全威胁

- 临时人员、供应商、合作人员（业务伙伴的员工）以及公众。
- 要求供应商和合作伙伴进行适当的审查和安全培训。
- 合同规定安全责任。
- 尽可能少地提供账号和密码，并尽快删除这些账号。

公众用户

- 网站和其他可公开访问的信息系统。
  - **硬化**
    - 操作系统的特殊版本。
    - 锁定或消除应用程序不需要的操作系统特征和功能。
  - 保护这些用户免受企业内部安全问题的影响。

账户管理

- 账户管理
  - 创建新用户账户、修改账户权限以及删除不需要的账户。
- 密码管理
  - 用户频繁地更改密码。
- 帮助平台政策
  - 提供用户身份认证的方法。

员工申明举例

本人特此确认以下列出的有关与用户 ID 关联的系统密码的个人职责。我知道我负责保护密码，将遵守所有适用的系统安全标准，并且不会向任何人泄露我的密码。我还知道，若我在使用密码时遇到问题或者我有理由相信密码的私人性质受到损害，我必须向信息系统安全官（information system security officer）报告。

图 10–8 员工申明举例

资料来源： National Institute of Standards and Technology, U.S. Department of Commerce. Introduction to Computer Security: The NIST Handbook, Publication 800–812.

系统处理规程

10-7 人员安全保障如何防范安全威胁

表 10-7 系统处理规程

	系统用户	运营人员
正常操作	使用系统完成工作任务，并保证安全性与敏感度相适应	操作数据中心设备，管理网络，运行 Web 服务器，并完成相关的操作任务
备份	为丢失系统功能做准备	备份 Web 站点资源和数据库，备份管理数据、账户和密码数据以及其他数据
恢复	在失败期间完成工作任务，并知道在系统恢复期间要做的任务	从备份数据中恢复系统，并在恢复期间承担帮助平台所应完成的工作

安全监控

- 服务器活动日志
  - 防火墙日志
    - 所有丢弃的数据包列表、渗透尝试以及来自防火墙的未经授权的访问尝试。
  - DBMS
    - 成功和失败的日志。
  - Web活动日志
    - 大量的Web活动日志。
- PC O/S produce record of log-ins and firewall activities.

安全监控（续）

- 使用工具来评估安全脆弱性。
- 蜜罐供计算机犯罪者攻击。
- 调查安全事件。
- 不断监测以确定现有的安全政策和安全保障是否足够。

事件响应的因素

10-8 组织应如何应对安全事件

表 10–8 事件响应的因素

• 有准备就绪的计划
• 集中报告
• 特定的响应
– 速度
– 准备工作将会带来回报
– 不要让问题变得更糟
• 演习

2017年的信息系统安全

10-9 2027?

- APT更加普遍。
- 关注国家安全和个人隐私之间的平衡。
- 设备的安全性将得到改善。
- 猫鼠活动技术水平大幅提高。
- 大型组织的安全性提高。
- 强大的本地“电子”警长。

彻底的欺骗

安全指南

- 员工（可能是管理者）制作欺骗性的软件用于欺骗标准化排放测试。
- 黑箱软件使得检测恶意软件变得困难。
- 嵌入式软件旨在：
  - 临时提高燃油节省量
  - 减少扭矩和加速度
- 当正常的性能恢复时，排放量的增长大大超过了法律水平。

IT安全分析师

就业指南

Stefanie at Overstock.com

Q. 什么吸引你进入这个领域？

A. “我第一次被IT安全领域吸引是作为一名大二的学生，那时候我参加了我最初的MIS课程。在一次会议中，教授部署了一个蜜罐，我们看到了攻击者在扫描系统漏洞。有太多扫描！我喜欢这样的想法：找到并阻止攻击者利用别人的利益。”

Q. 有什么建议可以给那些想在你这个领域工作的人呢？

A. “阅读，阅读，阅读！我看到很多潜在的分析师都在接受采访，因为他们没有基本的安全基础。”

章节回顾

10-1 信息系统安全的目标是什么
10-2 计算机安全问题有多大
10-3 个人应如何应对安全威胁
10-4 组织应如何应对安全威胁
10-5 技术安全保障如何防范安全威胁
10-6 数据安全保障如何防范安全威胁
10-7 人员安全保障如何防范安全威胁
10-8 组织应如何应对安全事件
10-9 2027？

击中塔吉特公司

案例研究10

- 丢失了4000万张信用卡和借记卡的号码。
- 随后，宣布另外还有7000万客户账户被盗，其中包括姓名、电子邮件、地址、电话号码等。
- 9800万客户受到影响。
  - 相当于美国3.18亿人中的32%。
- 是在假日购物季节从塔吉特公司的零售商店的销售点（POS）系统中被盗的。

他们怎么做到的

案例研究10

1. 购买恶意软件
2. 攻击者在塔吉特的供应商服务器上获取登录凭据
3. 攻击者升级了服务器的权限，获得了对塔吉特内部网络的访问权限，并植入恶意软件。
4. 恶意软件从POS终端提取信息。
5. 将数据发送到下一级服务器

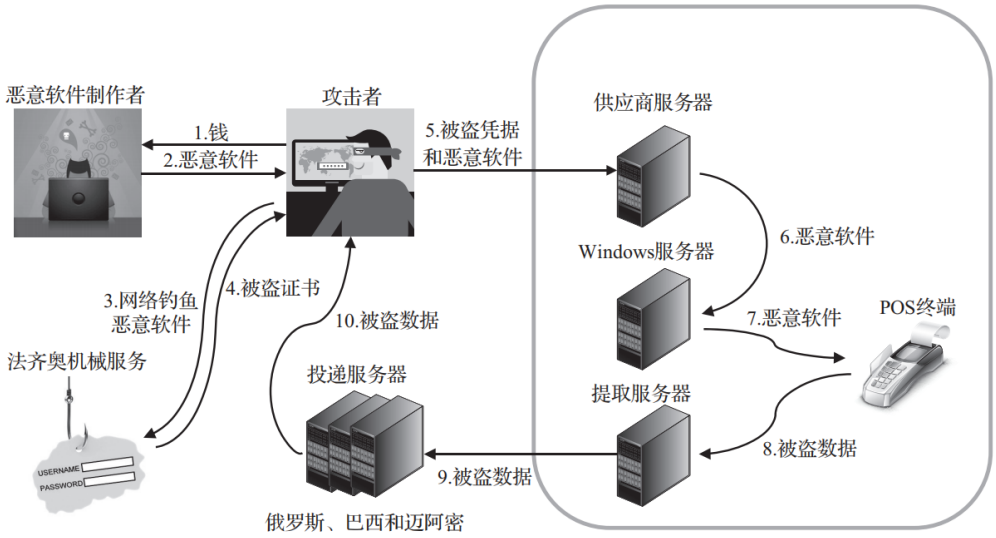


图 10–9　塔吉特公司的数据泄露

损害

案例研究10

- 攻击者售出约200万张信用卡，每张金额约为26.85美元，总利润为5370万美元。
- 花费
  - 升级POS终端以支持芯片和PIN卡，
  - 增加保险费，
  - 支付法律费用，
  - 解决信用卡处理器，
  - 为消费信贷监控付费，
  - 支付监管罚金。

损害（续）

案例研究10

- 客户信心的丧失和收入的下降（季度损失46%）。
- 直接损失高达4.5亿美元。
- 首席信息官辞职，并为首席执行官的离开支付1600万美元。
- 花费信用合作社和银行超过2亿美元用于发行新卡。
- 保险公司要求更高的保费，更严格的控制和更多的系统审计。
- 如果出现欺诈性收费，消费者必须查看信用卡账单，并填写书面文件。