第十九章 事件与道德规范

19.1 调查

- 所有信息安全专家迟早都要遇到调查的安全事件

19.1.1 调查的类型

- 操作型调查：涉及组织的计算基础设施问题，且首要目标为解决业务问题，操作型调查较为宽松，为了解决操作问题以及识别出现问题的根本原因，以防出现类似问题
- 犯罪调查：通常由执法者进行，针对违反行为进行的调查，犯罪过程必须遵守非常严格的证据收集和保存过程
- 民事调查：涉及内部员工和外部顾问代表法律团队的工作，采用较弱证据标准
- 监管调查：政府机构认为个人和企业可能违反法律时会执行监管调查
- 电子发现：保留与安全相关的证据，兵在控诉双方之间分享信息

19.1.2 证据

为了成功检举犯罪，起诉律师必须提供足够的证据来正视某个人的罪行超出合理的怀疑

1. 可接纳的证据
    - 可接纳的证据必须满足三点：
        - 证据必须与实施相关
        - 证据的实施必须对本案来说是必要的
        - 证据必须有法定资格，意味必须合法获得
2. 证据得了类型
    - 法庭可用的证据有四个类型
        - 实物证据：也叫客观证据，实物证据是直接证据，还可能是无可辩驳的结论性证据
        - 文档证据：所有带到法庭用于证明事实的书面内容，证据必须经过验证
    - 两种额外的证据被用用与文档证据
    - 最佳证据规则声明，必须为原始文档，原始证据的副本或说明不会被接受为证据
        - 言辞证据：包括证人证词，也可以是记录存储的书面证据，
        - 传闻证据：没有经过系统管理员验证的计算机日志文件可能被认为是传闻证据
3. 证据收集过程
    - 取证时，保留原来的证据可能很重要，分析数据时最好使用副本
    - 介质分析：介质分析是计算机取证分析的分支，包括磁介质、光学介质、存储器

- 网络取证分析：网络取证分析往往取决于对事件发生的预先了解，或使用记录网络活动的已存在的安全控制，如
  - 入侵检测和防御日志
  - 流量检测系统捕获的网络流量数据
  - 事件发生过程中有意收集的数据包
  - 日志、防火墙和其他网络安全设备
- 软件分析： 对软件及其活动进行检查
- 硬件/嵌入式设备分析：硬件和嵌入式设备分析需要专业的相关知识，掌握介质分析和软件分析

19.1.3 调查过程

- 请求执法：首要决定是，是否请求执法机构介入
- 实施调查：如果不请求执法机构的协助，应当试图遵守合理的调查原则，以确保调查的准确和公平

19.2 计算机犯罪的主要列别

- 攻击计算机系统有很多种方式，同事对计算机系统进行攻击的动机也有很多种

19.2.1 军事和情报攻击

- 主要用于从执法机构或军事和技术研究机构获得秘密和受限的信息

19.2.2 商业攻击

- 商业攻击专门非法获取公司机密信息

19.2.3 财务攻击

- 财务攻击被用于非法获得钱财和服务

19.2.4 恐怖攻击

- 恐怖攻击的目标是中断正常的生活和制造恐怖气氛，计算机恐怖攻击的目标可能是控制电厂、造成电力中断或控制电信

19.2.5 恶意攻击

- 恶意攻击的冬季通常来自不满，并且攻击可能是现在或以前的员工，认真的对系统漏洞进行监控和评估，是应对大多数恶意攻击的最佳防御措施

19.2.6 兴奋攻击

- 兴奋攻击是具有很少技能的破坏者发起的攻击，动机是闯入系统的及其兴奋

19.3 事故处理

- 事件：在特定时间周期内发生的任何事情
- 事故：对组织数据的机密性、完整性和可用性具有负面影响的事件

19.3.1 常见的事故类型

1. 扫描：仅扫描系统可能并不犯法，扫描是一种普遍现象，因此一定要自动收集证据
2. 泄密：系统或系统存储的信息进行的未授权访问
3. 恶意代码： 保护恶意代码的最有效方法就是使用病毒和间谍软件进行扫描并保持特征数据库最新
4. 拒绝服务攻击：最容易检测的事故类型

19.3.2 响应团队

- 负责调查计算机安全事故的专门团队

19.3.3 事故响应过程

1. 检测和确认
    - 确定事故以及通知适当的人员
2. 响应和报告
    - 一旦确定事故已发生，下一步就是选择恰当的行动
        - 隔离与抑制：致力于限制组织泄密和阻止进一步破坏
        - 收集证据： 为了执行适当的调查，没收设局、软件或数据时常有的事情
            - 拥有人资源交出证据
            - 法院传票或法令，强迫个人或组织交出证据，并由执法部门强制执行传唤
            - 让员工签署协议，使其同意在调查期间可搜寻和没收任何必要的证据
        - 分析和报告：收集完成证据，分析证据确定导致事故的一系列时间，并交给管理部门书面报告概述发现
3. 恢复和补救
    - 恢复：修正针对组织的所有已发生破坏，并限制将来由于类似事故导致的破坏
    - 总结经验教训：反思行为能够为今后成功的事故响应提供重要参考

19.3.4 约谈个人

- 约谈是一种专门得技巧，应当只由训练有素的调查人员进行

19.3.5 事故数据的完整性和保存

- 一定要确保能够维护所有证据的完整性，方法如：
  - 简单的归纳策略，有助于确保能够在需要时获得证据
  - 远程日志记录

19.3.6 事故报告

- 事故发生之前，与公司的法律人员或适当的执法代理机构建立良好的关系是非常明智的

19.4 道德规范

- 道德规范是对专业人士行为的最低标准

19.4.1 ISC的道德规范

- 保护社会、公益、必须的公信与自信，以及基础设施
- 行为得体、诚实、公正、负责和遵守法律
- 为委托人提供尽职的、胜任的服务工作
- 发展和保护职业

19.4.2 道德规范和互联网

- 不可接受和不道德的
  - 试图获得未经授权访问internet资源的权利
  - 破坏Internet正常使用
  - 通过这些行为耗费资源
  - 破坏以计算机为基础的信息的完整性
  - 危害用户的隐私权