第4章 信息安全策略管理

信息安全管理

主讲 李章兵

内容

- 1. 信息安全策略概述
- 2. 信息安全策略的制定
- 3. 信息安全策略管理

4.1 信息安全策略概述

- 1. 信息安全策略定义
  - 一种处理安全问题的管理策略的描述，是描述程序目标的高层计划。
    - 安全策略本质上是非形式化的,也可以是高度数字化的。
  - 信息安全策略是指在某个安全区域内，用于所有与安全相关活动的一套规则。
    - 一个安全区域，通常是指属于某个组织的一系列处理和通信资源。
    - 由安全区域所属的一个安全权力机构建立；
    - 由安全控制机构来描述、实施或实现。
  - 信息安全策略本质上是描述组织具有哪些重要信息资产，并说明其如何被保护的一个计划。

4.1 信息安全策略概述

- 2.信息安全策略的层次
  - (1).信息安全方针
    - 信息安全方针就是组织的信息安全委员会或管理机构制定的一个高层文件，用于指导组织如何管理、保护和分配信息资产 (包括敏感性) 的规则和指示。
      包括：
      - 信息安全的定义、总体目标和范围，安全对信息共享的重要性；
      - 阐述管理层的意图、支持目标和信息安全原则；
      - 简要说明信息安全的控制、依从法律法规要求对组织的重要性；
      - 定义信息安全管理的一般和具体责任、报告安全事故等。

4.1 信息安全策略概述

- 2.信息安全策略的层次
  - (2).信息安全策略规则
    - 是实施安全策略的程序；
    - 实施安全控制目标与控制方式的控制程序；
    - 为覆盖ISMS的管理与运作的程序。
- 3.安全程序
  - 程序是为进行某项活动所规定的途径或方法。
  - 安全程序是保障信息安全策略有效实施的、具体化的、过程性的措施。
    - 是信息安全策略从抽象到具体、从宏观管理层落实到具体执行层的重要一环。

4.1 信息安全策略概述

- **3.安全程序**
  - 安全程序文件应遵循的原则
    - 针对影响信息安全的各项活动目标做出的执行规定
    - 一般不涉及纯技术性的细节
    - 应当简练、明确和易懂
    - 应当采用统一的结构与格式编排
  - 程序文件的内容包括：
    - 活动的目的与范围（**Why**）
    - 做什么（**What**）
    - 谁来做（**Who**）
    - 何时（**When**）
    - 何地（**Where**）
    - 如何做（**How**）

4.1 信息安全策略概述

- 4. 信息安全策略分类
  - 保密性策略
  - 可用性策略
  - 完整性策略
  - 纵向上分：（略）
    - 总体安全策略
    - 针对特定问题的安全策略
    - 针对特定系统的具体策略

4.1 信息安全策略概述

- **4. 信息安全策略分类**
  - 横向分：（略）
    - 物理安全策略
    - 网络安全策略
    - 数据加密策略
    - 病毒防护策略
    - 数据备份策略
    - 身份认证及授权
    - 系统安全策略
    - 商业伙伴、客户关系策略
    - 灾难恢复策略
    - 事故处理紧急响应策略
    - 安全教育策略
    - 口令管理策略
    - 补丁管理策略
    - 系统变更控制策略
    - 复查审计策略

4.1 信息安全策略概述

- **5. 信息安全策略的作用**
  - 明确组织的重要资产及重要程度；
  - 明确如何安全使用和保护重要资产；
    - 明确组织的信息系统资源如何安全使用；
    - 明确如何处理敏感信息；
    - 明确如何采用安全技术产品。
- **6. 信息安全策略的意义**
  - 安全策略是在效率和安全之间的一个平衡点。
    - 先进的网络安全技术是网络安全的根本保证；
    - 严格的安全管理是确保信息安全策略落实的基础；
    - 严格的法律、法规是网络安全保障的坚强后盾。

4.2 安全策略的制定

- **1. 策略的制定时间**
  - 制定安全策略须在业务活动开始之前
    - 任何业务活动过程均有风险，应尽早制定安全策略
    - 无策略的开发、投资和责任都很大

4.2 安全策略的制定

- 2.安全策略制定原则
  - 三个基本原则
    - 确定性、完整性、有效性（还应有宏观性）
  - 起点进入原则
  - 长远安全预期原则
    - 从全局考虑，不要把风险孤立对待
  - 最小特权原则
  - 公认原则
    - 发生过一次的事故很可能会再次发生
  - 适度复杂与经济原则

4.2 安全策略的制定

- **3. 安全策略的保护对象**
  - 信息系统的硬件与软件
    - 随系统而变化
  - 信息系统的数据
    - 第三方数据的使用
    - 定义好隐私条例
  - 人员权限和公司行为的合法性
    - 安全策略将系统的状态分为两个集合:
      - 已授权的和未授权的。

4.2 安全策略的制定

- **3. 安全策略的保护对象**
  - 完整信息安全策略的覆盖范围

- 网络设备安全
- 服务器安全
- 信息分类
- 信息保密
- 用户账户与口令
- 远程访问
- 反病毒
- 防火墙及入侵检测
- 安全事件调查与响应
- 灾难恢复与业务持续性计划
- 风险评估
- 信息系统审计

4.2 安全策略的制定

- 4. 安全策略制定流程
  - (1)确定保护对象和原因
  - (2)制定安全策略的目标
  - (3)流程：
    - 确定策略范围
    - 风险评估、审计
    - 策略的审查、批准和实施

4.2 安全策略的制定

- 4. 信安全策略制定流程
- (1)管理层授权
  - 得到管理层的明确支持与承诺，使制定的安全方针、政策和控制措施可以在组织的上上下下得到有效的贯彻；
  - 可以得到有效的资源保证。
- (2)理解组织业务特征
  - 使制定的信息安全策略与组织的业务目标一致。

4.2 安全策略的制定

- **(3)组建安全策略制定小组**
  - 高级管理人员；
  - 信息安全管理员；
  - 信息安全技术人员；
  - 负责安全策略执行的管理人员；
  - 用户部门人员。
- **(4)确定信息安全整体目标**
  - 通过防止和最小化安全事故的影响，保证业务持续性，使业务损失最小化，并为业务目标的实现提供保障。

4.2 安全策略的制定

- **(5)确定安全策略范围和保护对象**
  - 根据实际情况确定信息安全策略的范围
    - 整个组织
    - 个别部门
    - 个别领域。
  - 安全策略涉及的问题
    - 敏感信息如何被处理？
    - 如何正确地维护用户身份与口令，以及其他账号信息？
    - 如何对潜在的安全事件和入侵企图进行响应？
    - 如何以安全的方式实现内部网及互联网的连接?
    - 怎样正确使用电子邮件系统？

4.2 安全策略的制定

- **(6)风险评估与选择安全控制**
  - 风险评估的结果是选择适合组织的控制目标与控制方式的基础；
  - 组织选择出了适合自己安全需求的控制目标与控制方式后，安全策略的制定才有了最直接的依据。
- **(7)起草拟定安全策略**
  - 安全策略要尽可能地涵盖所有的风险和控制，没有涉及的内容要说明原因；
  - 阐述如何根据具体的风险和控制来决定制订什么样的安全策略。

4.2 安全策略的制定

- **(8)评估安全策略**
  - 合规性：安全策略是否符合法津、法规、技术标准及合同的要求?
  - 有效性：安全策略是否满足组织在各个方面的安全要求?
  - 授权：管理层是否已批准了安全策略，并明确承诺支持政策的实施?
  - 适用性：
    - 安全策略是否损害组织、组织人员及第三方的利益?
    - 安全策略是否实用、可操作并可以在组织中全面实施?
    - 安全策略是否已传达给组织中的人员与相关利益方，并得到了他们的同意？

4.2 安全策略的制定

- **(9)定稿与审批**
  - 制定小组定稿后提交管理层
  - 管理层审批
    - 策略文件的确定性、完整性、有效性；
    - 策略文件的可行性、合法性。
  - 有效的信息安全策略的特点
    - 满足大部分需求并能够维护组织、企业的利益
    - 策略应该清晰但不能包含太多的细节
    - 策略应该不断加强
    - 策略的目标应该整合到员工培训课程中去

4.3 安全策略的管理

- **1.安全策略管理办法**
  - 集中式管理
    - 在整个网络系统中，由统一、专门的安全策略管理部门和人员对信息资源和信息系统使用权限进行计划和分配。
  - 分布式管理(责任下沉)
    - 将信息系统资源按照不同的类别进行划分，然后根据资源类型的不同，由负责此类资源管理的部门或人员负责安全策略的制定和实施。

4.3 安全策略的管理

- **2.安全策略管理相关技术**
  - 安全策略统一描述技术
    - 安全策略描述是实现策略管理的基础。
    - 策略描述语言：**PDL、Ponder**。
  - 安全策略自动翻译技术
    - 安全策略翻译是指将统一描述的安全策略翻译成不同设备对应的配置命令、配置脚本或策略结构的过程。
  - 安全策略一致性检验技术
    - 策略之间的冲突很难避免。
    - 策略一致性验证主要包括策略的语法、语义检查和策略冲突检测两个方面。

4.3 安全策略的管理

- **2.安全策略管理相关技术**
  - 安全策略发布与分发技术
    - 把安全方针与具体安全策略编制成组织信息安全策略手册，然后发布到组织中的每个组织人员与相关利益方。
    - “推”模式
    - “拉”模式
  - 安全策略状态监控技术
    - 策略的生命周期状态包括：
      - 休眠态、待激活态、激活态、挂起态。

4.3 安全策略的管理

- **3.信息安全策略的执行**
  - 发布安全策略
  - 落实责任人员
  - 责任声明和监控制度是最重要的保证

4.3 安全策略的管理

- **4.安全策略的持续改进**
  - 组织所处的内外环境在不断变化；
  - 信息资产所面临的风险也是一个变数；
  - 人的思想和观念也在不断的变化。
    - 几乎所有层次的所有人员都会涉及到这些政策；
    - 组织中的主要资源将被这些政策所涵盖；
    - 将引入许多新的条款、程序和活动来执行安全策略。
  - **审查和修订周期6个月或1年。**

4.4 主要信息安全策略

- **1.口令策略**
  - 总体要求 难以破解易于牢记
  - **(1)网络服务器的口令管理**
    - 部门负责人和网络管理员同时在场设定
    - 系统管理员记录封存
    - 定期更换并销毁原记录封存新记录
    - 发现泄密及时报告、保护现场，须接到上一级主管部门批示后再更换口令

4.4 主要信息安全策略

- **1.口令策略**
  - **(2)用户口令管理**
    - 用户负责人与系统管理员商定口令，负责人确认，管理员登记、存档
    - 用户要求查询或更换口令需提交申请单
    - 网络提供用户自我更新口令功能时，用户应自行定期更换并设专人负责保密和维护
  - **(3)创建口令规则**
    - 通用规则
      - 保存口令最安全的地方是脑袋和保险箱
      - 口令需相当长
      - 以合理的方式使用特殊字符、大写字母、数字

4.4 主要信息安全策略

- **1.口令策略**
  - **(4)需避免的问题**
    - 不要用个人信息
    - 不用自己的偶像信息
    - 不用办公桌（室）上的物品
    - 不将口令保存在本地机器或共享的网络上

4.4 主要信息安全策略

- **2.计算机病毒和恶意代码防治策略**
  - 防护策略须遵守的准则
    - 拒绝访问能力
      - （来历不明软件不得进入）
    - 病毒检测能力
      - （能否检测病毒是重要指标）
    - 控制传播能力
    - 清除能力
    - 恢复能力
    - 替代操作

4.4 主要信息安全策略

- 3.用户安全策略内容（略）
  - 数据和用户所有权（数据的专用和共享）
  - 硬件的使用（明确正确的操作方式）
  - 互联网的使用（正确的使用方式）
  - 帐户管理、补丁管理、事件报告制度（管理员）
  - 策略更新
  - 强制执行策略（保障）

4.4 主要信息安全策略

- **4.安全教育与培训策略**
  - 安全教育的层次性
    - 管理人员：企业信息安全的整体策略和目标，信息安全体系的构成、部门建立和制度完善
    - 技术人员：理解策略、掌握评估方法，合理运用安全操作和维护技术
    - 用户：学习操作流程、了解掌握安全策略
  - 安全教育与培训策略举例
    - 建立专门的安全教育与培训机构
    - 制定详细的安全教育和培训计划
    - 定期对教育和培训结构进行抽查和考核

小结

- 信息安全策略是指在某个安全区域内用于所有与安全相关活动的一套规则。一种处理安全问题的管理策略的描述，是描述程序目标的高层计划。
- 制定安全策略须在业务活动开始之前
- 安全程序是保障信息安全策略有效实施的、具体化的、过程性的措施，是信息安全策略从抽象到具体，从宏观管理层落实到具体执行层的重要一环。
- 安全策略的保护对象：硬件与软件、数据、人员
- 安全策略制定流程:确定保护对象和原因、目标、策略范围；风险评估、审计；策略的审查、批准和实施。