第7章 信息安全策略

信息安全工程与实践

- 本章学习目标
  - 掌握信息安全策略的基本概念和制定原则。
  - 掌握信息安全策略的规划和实施方法。
  - 了解常见的信息安全策略。
  - 了解备份与恢复策略。

7.1 信息安全策略概述

- 信息保障强调信息安全的保护能力，同时重视提高系统的入侵检测能力、事件响应能力和快速恢复能力，关注的是信息系统整个生命周期的保护、检测、响应和恢复等安全机制，即PDRR安全模型。

7.1 信息安全策略概述

- PPDR模型：美国ISS公司提出的动态网络安全体系的代表模型，也是动态安全模型的雏形。

- PPDR模型与PDRR模型都是重要的动态防御模型，强调网络信息系统在受到攻击的情况下，网络系统的稳定运行能力。

7.1 信息安全策略概述

- PPDR：Policy、Protection、Detection、Response
- Policy：模型的核心。防护、检测和响应是根据安全策略实施的。
- Protection：根据系统可能出现的安全问题而采取的措施。
- Detection：攻击者穿透防护系统时，检测发挥作用。检测是动态响应的依据。
- Response：事件处理。包括应急响应和灾难恢复。

7.1 信息安全策略概述

信息安全策略的概念

- PPDR模型是在整体的安全策略的控制和引导下，在综合运用防护工具的同时，利用检测工具了解和评估系统的安全状态，通过适当的反应将系统调整到“最安全”和“风险最低”的状态。防护、检测和响应组成了一个完整的、动态的安全循环，在安全策略的指导下保证信息系统的安全。
- PPDR模型是基于时间的安全理论为基础。
- 提高系统的防护时间；
- 降低检测时间和响应时间。

7.1 信息安全策略概述

信息安全策略的概念

- 信息安全策略，是一个有效的信息安全项目的管理基础。它规定了所允许的访问控制、协议以及如何面对与安全有关的事件。
- 信息安全策略，已成为PPDR（P2DR）模型的核心。
- 安全策略是整个网络信息安全的依据。不同的网络需要不同的安全策略。

7.1 信息安全策略概述

信息安全策略的概念

- 计算机安全研究组织SANS描述：
  - 为了保护存储在计算机中的信息，安全策略要确定必须做什么，一个好的策略有足够多‘做什么’的定义，以便于执行者确定‘如何做’，并且能够进行度量和评估。
  - 一组规则，这组规则描述了一个组织要实现的信息安全目标和实现这些信息安全目标的途径。
  - 信息安全策略提供：信息保护的内容和目标，信息保护的职责落实，实施信息保护的方法，事故的处理。

7.1 信息安全策略概述

信息安全策略的格式

- 目标
- 范围
- 策略内容
- 角色责任
- 执行纪律
- 专业术语

7.1 信息安全策略概述

信息安全策略的保护对象

硬件与软件	硬件和软件是支持商业运作进行的平台，它们应该受策略所保护。所以，拥有一份完整的系统软、硬件清单是非常重要的，并且包括网络结构图
数据	计算机和网络所做的每一件事情都造成了数据的流动和使用，所有的企业、组织和政府机构，不论从事什么工作，都在收集和使用数据
人员	首先，重点应该放在谁在什么情况下能够访问资源，接下来要考虑的就是强制执行制度和对未授权访问的惩罚制度
备份、文档存储和数据处理	把数据备份到外部站点或者其他介质上，有关这方面的策略和在线访问信息策略是同样重要的。备份数据可以包括财政信息、客户往来记录甚至当前业务过程的复制。备份策略需要考虑的情况包括：数据如何存档，在准备丢弃数据的时候应该做些什么

7.1 信息安全策略概述

信息安全策略的意义

- 信息安全策略是一个有效的信息安全项目制定的必要基础
- 信息安全策略的制定和实施决定了任何一个信息安全项目的成功
- 改善了信息安全管理的可扩展性和灵活性是应用信息安全策略的主要优势

7.2 信息安全策略的内容

信息安全策略的分类

- 总体安全策略（或企业信息安全策略）
- 问题安全策略
- 功能安全策略

7.2 信息安全策略的内容

总体安全策略1——要求

- 总体安全策略,是从整体上为组织机构的安全工作制定战略方向、范围和策略基调:
  - 为信息安全的各个领域分配责任，包括信息安全策略的维护、策略的实施、最终用户的责任等。
  - 规定信息安全项目的制定、实施和管理的安全控制要求。
- 应支持组织的预定目标和任务声明，而不能相互抵触。

7.2 信息安全策略的内容

总体安全策略2——组成要素

- 关于组织安全理念的总体看法。
- 组织的信息安全部门结构和实施信息安全策略人员的信息。
- 组织所有成员共同的安全责任。
- 组织所有成员明确的、特有的安全责任。

7.2 信息安全策略的内容

总体安全策略3——组成框架

组成部分	描 述
目的声明	确定全面的安全策略和方向
信息技术的安全要素	定义受保护信息的保密性、完整性、可用性等而采取的各类措施，包括技术控制策略、教育和培训等
信息安全的必要性	强调信息安全的重要性，明确保护重要信息安全的法律和道德责任
相关角色和责任	定义支持信息安全的组织结构，明确各类机构成员的信息安全责任
相关参考标准	列出影响安全策略的相关法律、法规、标准和其他策略

7.2 信息安全策略的内容

问题安全策略1——要求

- 问题安全策略,是为组织成员如何使用基于技术的信息系统提供了详细的、目标明确的指南。
- 明确指出组织期望员工如何使用基于技术的信息系统。
- 确定并记录基于技术的信息系统的控制过程。
- 当由于员工的使用不当或非法操作而造成的损失，组织不为其承担责任。

7.2 信息安全策略的内容

问题安全策略2——组成要素

目标声明	策略的范围、服务目标和适用性；定义所涉及的技术；实施策略的责任
访问授权和使用设备	用户是否可以访问资源、公正和负责任地使用资源、对个人信息和隐私的保护
禁止使用设备	破坏性地使用或误用、冒犯或侵扰设备运行、侵犯版权、未经批准的或用于其他目的犯罪活动
系统管理	储存介质的管理、授权监控、病毒防护、信息加密、物理安全、用户和系统管理员的责任
违反策略	通报违规的过程、对违规的惩罚
策略检查和修改	定期检查过程和时间表、修改的过程
责任声明	责任的声明、拒绝对某些行为承担责任

7.2 信息安全策略的内容

功能安全策略

- 功能安全策略，是在配置和维护系统的时候起到标准和过程指导的作用。例如针对网络防火墙的功能配置和技术操作规程的策略。
  - 管理指南：主要是用来表明功能安全策略的技术要求。
  - 技术规范：指出具体的安全策略的技术实现方法。

7.2 信息安全策略的内容

功能安全策略2——技术规范

- 可能需要制定不同的技术策略来实现管理指南的安全要求，表现为各种不同的设备都具有独自的技术规范，用于实现将管理目标变为可以实施的技术方法。

7.2 信息安全策略的内容

功能安全策略2——技术规范

- 用以实现管理指南的技术控制规范有两种：
  - 访问控制列表（ACLs）。
  - 配置规则。

7.2 信息安全策略的内容

功能安全策略2——技术规范之访问控制列表

- 访问控制列表，包括用户访问列表、矩阵和权限列表等，控制用户的权限和特权，控制对系统功能、文档存储系统、中间设备或其他网络设备的访问。
- 权限控制列表详细规定了哪些设备、功能操作可以让哪些用户访问或执行等方面的内容，例如：
  - 授权谁可以使用系统。
  - 授权用户在何时何地可以访问什么。
  - 授权用户怎样访问系统，包括读、写、创建、修改、删除、拷贝等。

7.2 信息安全策略的内容

功能安全策略2——技术规范之访问控制列表

- Windows ACL：

7.2 信息安全策略的内容

功能安全策略2——技术规范之访问控制列表

- 配置规则，是输入到安全系统中指定的系统或设备的配置脚本或代码。这些代码在具体的系统或设备上执行，用来实现特定的安全功能，
- 配置脚本以代码形式存在，以用户界面方式接受管理员的配置规则要求，在系统底层转换为系统或设备可以接受并执行的代码。

7.2 信息安全策略的内容

物理和环境安全策略

- 安全区域
  - 根据信息安全的分层管理，将支持涉密信息或关键业务活动的设备放置在安全区域中
- 设备安全
  - 对支持涉密信息或关键业务过程（包括备份设备和存储过程）的设备应该适当地在物理上进行保护以避免安全威胁和环境危险

7.2 信息安全策略的内容

物理和环境安全策略

- 物理访问控制
  - 信息安全管理部门应建立访问控制程序，控制并限制所有对计算机及信息系统计算、存储和通信系统设施的物理访问
- 建筑和环境的安全管理
  - 为确保计算机处理设施能正确的、连续的运行，应至少考虑及防范以下威胁：偷窃、火灾、温度、湿度、水、电力供应中断、爆炸物、吸烟、灰尘、振动、化学影响等

7.2 信息安全策略的内容

物理和环境安全策略

- 保密室、计算机房访问记录管理
  - 保密室、计算机房应设立物理访问记录，信息安全管理部门应定期检查物理访问记录本，以确保正确使用了这项控制

7.2 信息安全策略的内容

计算机和网络运行管理策略

- 制定管理和操作所有计算机和网络所必需的职责和规程
- 控制对信息处理设施和系统的变动
- 对计算机介质进行控制，必要时使用物理保护
- 鉴别和网络安全（人员、设备、网络连接、网络服务、网络拓扑结构等的鉴别）
- 操作人员应保留日志记录

7.2 信息安全策略的内容

计算机和网络运行管理策略

- 对错误及时报告并采取措施予以纠正
- 确保网络信息可用性、数据安全性、网络服务的有效性，避免非法访问
- 计算机和信息系统应制定有关使用电子邮件的策略（数字签名策略、加密策略、生物识别策略）
- 预防和检查病毒（包括实时扫描/过滤和定期检查）
- 确定需要备份的内容、备份时间以及备份方式，建立有效的备份、恢复机制

7.2 信息安全策略的内容

风险管理及安全审计策略

- 定期执行计算机及信息系统的信息安全审计活动和风险评估
- 信息安全审计应当 3 个月进行一次，并形成文档化的信息安全审计报告
- 信息安全风险评估应当至少每年一次
- 必须形成文档化的风险评估报告

7.3 信息安全策略的制定过程

制定原则

- 不同的信息系统采取不同的安全策略，同时要考虑安全策略的控制成本、策略本身的安全保障以及策略的可靠性与业务的灵活性等方面的平衡。制定信息安全策略时，遵循以下原则：
  - 需求、威胁、风险与代价的平衡原则。
  - 安全可靠性与业务灵活性的平衡原则。
  - 完整性原则。
  - 易操作性原则。
  - 可评估性原则。
  - 坚持动态性。

7.3 信息安全策略的制定过程

制定流程

- 安全策略的制定以系统工程建设来对待，系统开发的生命周期是实现这一目标的途径。当进行一项安全策略的制定工程时，可以用SDLC过程对其进行指导：
  - 调查与分析阶段。
  - 设计阶段。
  - 实施阶段。
  - 维护阶段。

7.3 信息安全策略的制定过程

制定流程

- 调查与分析阶段
  - 组建安全策略制定小组。
  - 理解组织的企业文化和业务特征。
  - 获得管理层的支持与承诺。
  - 确定信息安全策略的目标和范围。
  - 相关资料的收集与分析。

7.3 信息安全策略的制定过程

制定流程

- 设计阶段
  - 起草拟定安全策略
    - ✓ 应确保策略的可实施性和可读性
  - 测试与评审安全策略
    - ✓ 对策略进行修改是必要的。

7.3 信息安全策略的制定过程

制定流程

- 实施阶段
  - 由管理层正式批准实施。应确保安全策略能顺利地发布到每个员工与相关利益方，并得到正确地理解，明确各自的安全责任与义务。
  - 要注意安全策略的发布与宣传工作。宣传安全策略形成良好的企业安全文化氛围。

7.3 信息安全策略的制定过程

制定流程

- 维护阶段
  - 针对瞬息万变的内外环境，组织应当实时监控、定期评审、调整和持续改进安全策略，以确保其始终是对付威胁变化的有效工具。

7.3 信息安全策略的制定过程

组织的安全策略

- 完整的信息安全策略组织应该有一个完整的信息安全策略
  - 适用范围：包括人员和时间上的范围
  - 目标
  - 策略主体
  - 策略签署
  - 策略的生效时间和有效期（或者重新评审时间）
  - 重新评审策略的时机
  - 与其他相关策略的引用关系
  - 策略解释、疑问响应的人员或者部门
  - 策略的格式

7.3 信息安全策略的制定过程

信息安全策略的主体内容

- 环境和设备的安全
- 信息资产的分级和人员责任
- 安全事故的报告与响应
- 第三方访问的安全性
- 委外处理系统的安全
- 人员的任用、培训和职责
- 系统策划、验收、使用和维护的安全要求

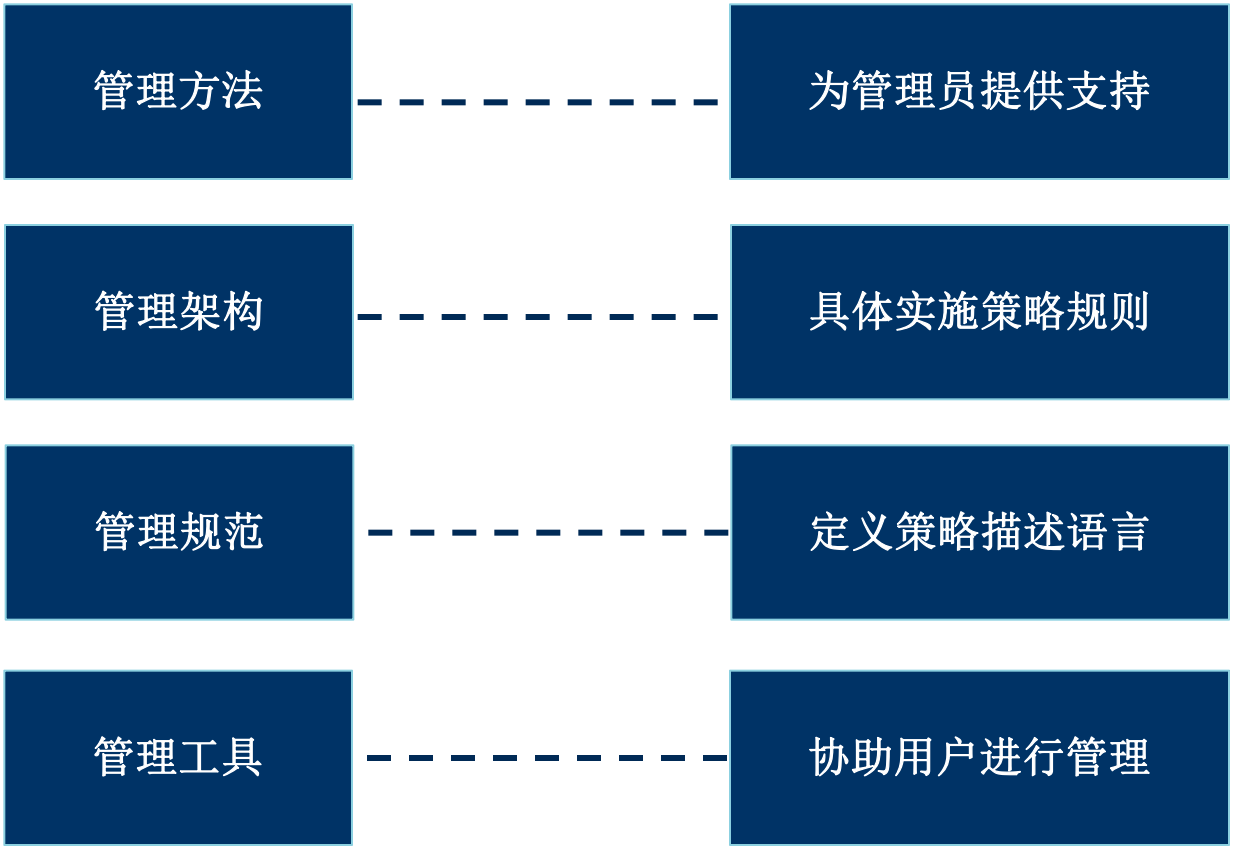
7.3 信息安全策略的制定过程

信息安全策略的主体内容

- 信息与软件交换的安全
- 计算级和网络的访问控制和审核
- 远程工作的安全
- 加密技术控制
- 备份、灾难恢复和可持续发展的要求
- 符合法律法规和技术指标的要求

7.4 安全策略实施与管理

- 完整的策略管理框架包括 4 个组成部分：**为管理员提供的策略系统管理方法、具体实施策略规则的策略管理架构、定义策略描述语言的策略规范以及为协助用户进行管理的策略管理工具。**

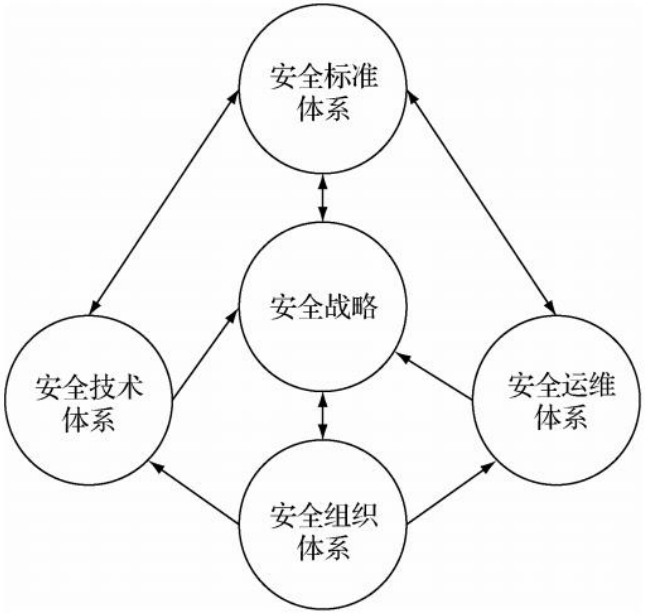


7.4 安全策略实施与管理

策略管理方法

✦集中式管理

- 集中式管理就是在整个网络系统中，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。



7.4 安全策略实施与管理

策略管理方法

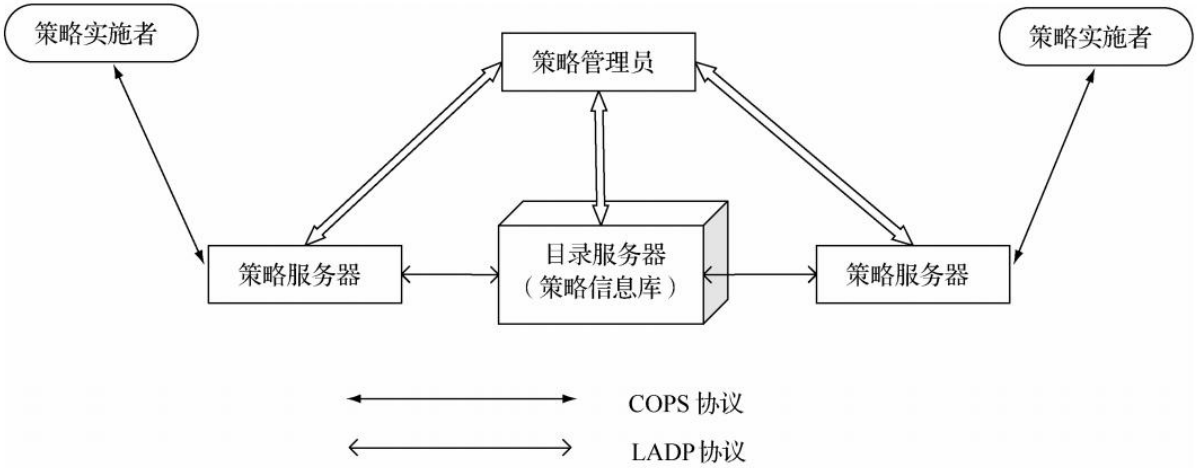
✦分布式管理

- 分布式管理就是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。
- 分布式管理访问模型的使用应遵循以下原则：
  - ✓ 通用性
  - ✓ 标准化
  - ✓ 兼容性
  - ✓ 最小信任域原则
  - ✓ 组件远程调用和异步通知
  - ✓ 策略自管理

7.4 安全策略实施与管理

策略管理架构

✦IETF 策略管理架构



策略管理架构中包括 4 个组件：策略服务器（也称策略决定点， PDP），策略管理员、目录服务器（也称策略信息库）和策略实施者（PEP）

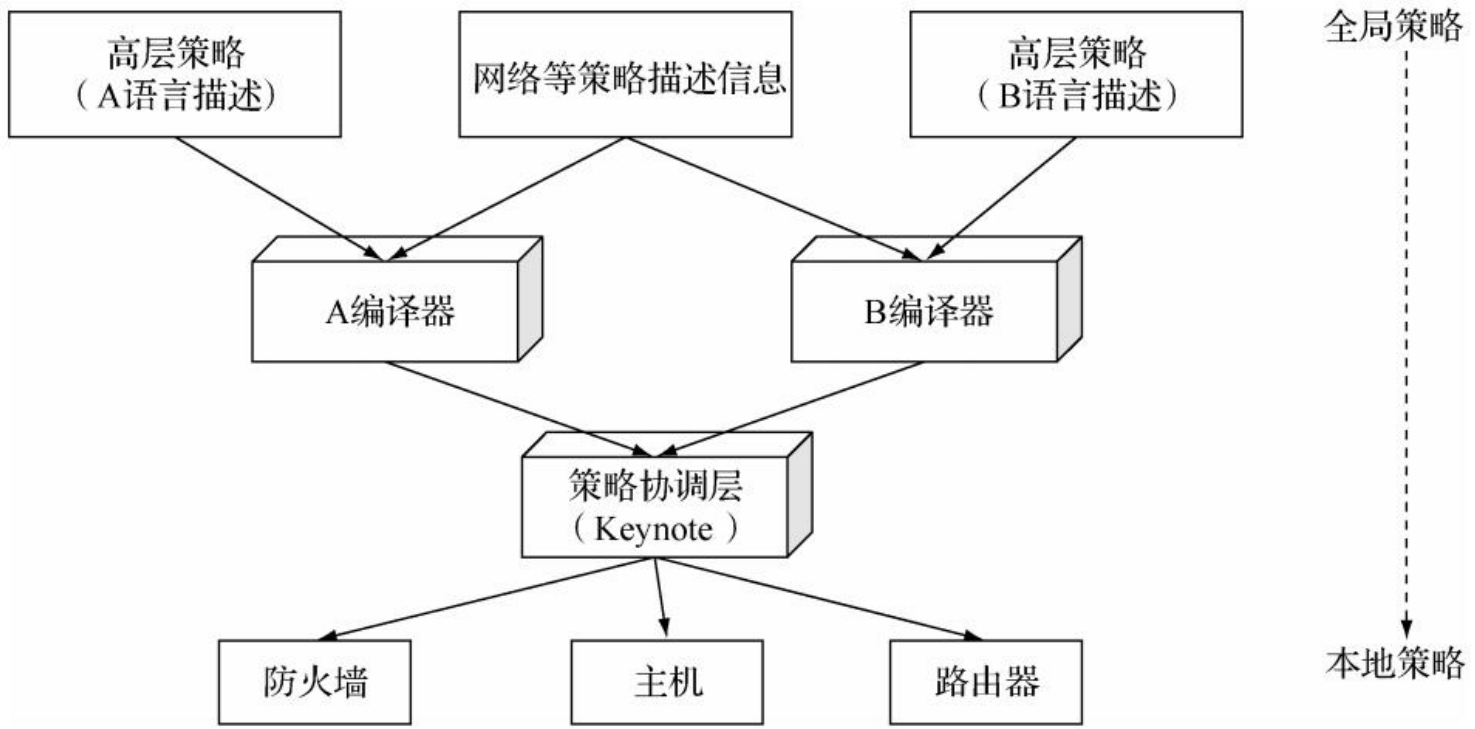
LDAP 协议：
LDAP 协议遵循 X.500 协议数据模式，实现 PDP 对目录服务器中策略信息的存取操作

COPS 协议： COPS 协议描述了一个基于信令协议的 QOS 策略控制客户/服务器模型，在 PDP 及其客户 （PEP）之间交换策略请求和决定信息。

7.4 安全策略实施与管理

策略管理架构

✦安全策略架构



7.4 安全策略实施与管理

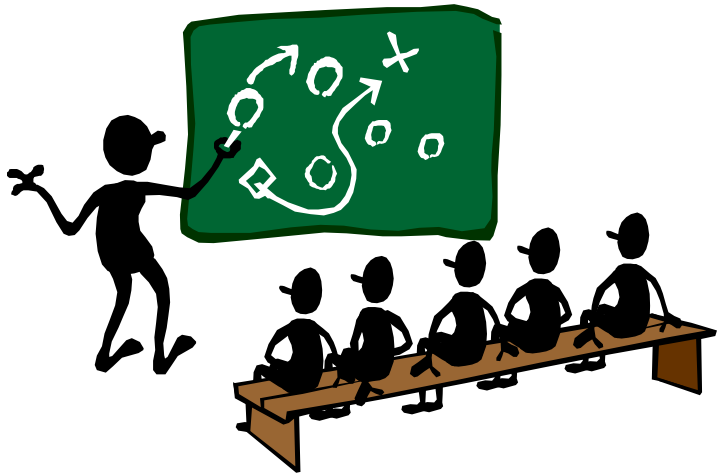
策略规范

- 策略规范定义了策略描述语言的语义和语法，可以划分为三层：
  - 高层抽象策略（也称管理目标），可以是比较抽象的商务目标，或者是服务等级约定（Service Level Agreements）、信任关系（Trust Relationships），甚至可以是自然语言的陈述
  - 规范层策略，指的是网络级或是商务级的策略，通常是由管理员人为制定的，这些信息安全策略策略与特定的服务有关，是对底层策略的抽象
  - 底层策略，也就是配置策略，通常是对特定的设备或是安全机制进行配置 （例如访问控制列表、防火墙规则等）

7.4 安全策略实施与管理

策略管理工具

- 策略管理工具：是操作策略管理系统的接口。
- 分为两种：通用管理工具和商用管理工具。



小 结

1. 安全策略是一个有效的信息安全项目的管理基础，是PPDR模型的核心，规定了所允许的访问控制、协议以及如何面对与安全有关的事件。
2. 分为:总体安全策略、问题安全策略和功能安全策略。
3. 制定安全策略时，可以用SDLC过程对其进行指导，并要考虑到一些原则。
4. IETF的策略管理框架与具体的实现技术无关，是一个可扩展的通用模型。
5. 在信息安全工程与管理项目中，应当摒弃一些偏见，按照标准和规范，认真地对待信息安全策略。

作 业

1. 信息安全策略的制定过程是怎样的?
2. 信息安全策略管理有哪些相关技术？这些技术的功能和作用分别是什么?
3. 信息安全策略是什么？它有何特点?
4. 如何进行信息安全策略的规划与实施?
5. 信息安全策略使用了哪些主要技术?

作 业

6．什么是环境安全策略？环境安全策略包括哪些方面的内容？

7．系统安全策略的目标是什么？包括哪些内容？

8．病毒防护策略的功能有哪些？有什么要求？

9．什么是安全教育策略？

10．信息安全策略在实际网络管理中有哪些体现？

实 验

实验五 基于信息安全策略的网络防火墙报文解析

实验六 基于信息安全策略的网络防火墙流量统计

实验七 网络安全扫描工具 Nessus 的使用

实验八 简单网络扫描器的设计与实现