# 管理信息系统 第四部分

2019年6月23日 18:32

## 信息系统管理

**第十章 信息系统安全**

1. 信息系统安全的目标
    a. 威胁/损失
        i. 威胁：未经所有者许可且通常在所有者不知道的情况下，寻求非法途径获取或更改数据或其它信息系统资源的个人或组织
        ii. 脆弱性：获得个人或组织资产的威胁机会
        iii. 保障：个人或组织采取的组织资产收到威胁的措施
    b. 威胁的来源
        i. 人为失误
        ii. 计算机犯罪
        iii. 自然事件和灾害
    c. 存在哪些类型安全损失
        i. 未经授权数据泄露
            1) 假托/欺骗：某人假装成另一个人骗人
            2) 网络钓鱼/电子邮件欺骗：通过使用假托电子邮件获取未经授权数据的技术
            3) 嗅探：拦截计算机通信的技术
                a) 战争驾驶者只需通过一个区域并搜索未受保护的无线网络，可以将计算机连接到无线网络
                b) 使用数据包嗅探器，捕获网络流量的程序
            4) 黑客
        ii. 不正确的数据修改
        iii. 服务错误
            1) 篡夺：计算机犯罪分子入侵计算机系统并用自己的未经授权的程序替换合法程序
        iv. 拒绝服务
        v. 基础设施缺失
2. 计算机安全问题有多大（p349-350阅读材料，超级大）
3. 个人如何应对安全威胁
    a. 列举几个个人安全保障措施p351
    b. 入侵检测系统：一种检测是否有另一台计算机试图扫描或访问计算机网络的系统
    c. 小心密码穷举法
    d. 定期删浏览器缓存
4. 企业如何应对安全威胁

a. 从五元模型出发
    i. 硬件和软件
        1) 识别和认证
        2) 加密
        3) 防火墙
        4) 恶意软件防护
        5) 应用设计
    ii. 数据
        1) 数据权利和义务
        2) 密码和加密
        3) 备份和恢复
        4) 物理安全
    iii. 处理规程和人员
        1) 处理规程设计
        2) 人员的雇佣，训练，教育，管理，评估，遵守，义务

5. 技术安全保障如何方法安全威胁
    a. 识别和认证
        i. 智能卡、个人识别号码PIN
        ii. 生物认证
    b. 多系统单点登陆
    c. 加密
        i. 加密算法
        ii. 密钥
        iii. 对称加密和非对称加密
        iv. 公开密钥加密
        v. 最安全的通信：https，使用安全套接层SSL协议加密，该协议也成为传输层安全，使用公开密钥加密和对称密钥加密
    d. 防火墙：防止未经授权的网络访问计算设备
        i. 边界防火墙
        ii. 内部防火墙
        iii. 包过滤防火墙：检查消息的各个部分，并确定是否让该部分通过，为了做出这个决定，检查源地址、目标地址和其它数据
    e. 恶意软件防护
        i. 病毒：可自我复制的计算机程序
            1) 有效载荷
        ii. 木马：伪装成有用的程序或文件病毒
        iii. 蠕虫：利用互联网或其它计算机网络自我传播的病毒
        iv. 间谍软件
            1) 键盘记录器
        v. 广告软件

vi. 勒索软件

f. 安全应用程序的设计

i. 比如如何防范SQL注入攻击

6. 数据安全保障如何防范安全威胁

a. 数据安全保障：保护数据库和其他组织数据

i. 明确数据政策

ii. 数据权利和责任

iii. 由密码认证的用户账户执行权限

iv. 数据加密

v. 备份和恢复程序

vi. 物理安全

b. 数据管理：开发和实施数据政策和标准的组织范围的功能

7. 人员安全保障如何防范安全威胁

a. 员工的人员安全保障

i. 职位定义

ii. 招聘和审查

iii. 宣传和执行

iv. 离职

b. 非员工人员安全保障

c. 账户管理

i. 账户管理

ii. 密码管理

iii. 帮助平台政策：忘了密码致电帮助平台，但不知道是不是真人。

iv. 系统处理规程

v. 安全监控

1）蜜罐：供计算机犯罪者攻击的虚假目标

8. 如何应对安全事件

a. 有准备就绪的计划

b. 集中报告

c. 特定的响应

i. 速度

ii. 准备工作会有汇报

iii. 不要让问题变糟糕

d. 演习

9. 2027

a. 计算机犯罪

**最后一章！12章 信息系统开发**

1. 如何开发业务流程、信息系统和应用程序

a. 业务流程、信息系统以及应用程序之间的区别与联系

i. 业务流程、信息系统和应用程序都有各自不同的特征和组件
ii. 业务流程和信息系统间的联系是多对多联系或N:M,一个业务流程不必与每个信息系统联系，但一个信息系统至少与一i个业务流程联系
iii. 每个信息系统都有一个软件组件，所以每个信息系统都至少包括一个应用程序

b. 不同开发过程适应场景有哪些
i. 探索三种开发过程：业务流程管理（BPM），系统开发生命周期（SDLC）以及scrum，（第四种叫窃取产品)
ii. 业务流程管理：用于创建新的业务流程和管理现有流程变化的技术
iii. 系统开发生命周期：用于开发信息系统和应用程序的过程
iv. Scrum:他的提出部分是为了解决SDLC的问题
v. 业务分析师、系统分析师

2. 如何使用业务流程管理
a. 业务流程：一个为实现某个业务功能而进行的交互活动、资源库、角色、资源的流组成的网络
i. 流要么是控制流，要么是数据流

b. 流程为什么要管理
i. 提高流程质量
ii. 适应技术变化
iii. 适应业务基础变化

c. BMP活动有哪些
i. 建模过程
ii. 创建组件
iii. 实施过程
iv. 评价结果
1）信息及相关技术的控制目标（COBIT)

3. 业务流程建模与标注如何应用于建模过程
a. 四阶段最重要的：建模过程
b. 业务流程标注的标准需求
i. 对象管理组织（OMG)的软件行业标准化组织建立了标准术语和图形符号，叫做业务流程建模与标注

c. 记录现行业务订单流程
i. 泳道布局

4. 系统开发声明周期有哪些阶段
a. 定义系统
i. 定义目标和范围
ii. 评估可行性
1）成本可行性
2）进度可行性
3）技术可行性

4) 组织可行性

iii. 组建项目团队

b. 确定需求

i. 需求来源

ii. 原型的角色

iii. 获得用户批准

c. 设计系统组件

d. 实施系统

i. 测试

ii. 系统切换

1) 试点安装：意味着组织只需要在企业种某个局部有限的安装整个系统

2) 分阶段安装

3) 并行安装：新系统/业务流程与旧系统/业务流程并行运行，直到新的全面投入运行

4) 插入安装，关闭旧的，启用新的

iii. 维护系统

1) 记录变化请求

a) 错误、改善

2) 按请求优先级排序

3) 修复错误

a) 找补丁

b) 服务包

c) 发新版本

5. 系统开发声明周期成功的关键因素是什么

a. 影响成功的五个关键因素

i. 建立一个工作分解结构

ii. 评估时间和成本

iii. 制定一个项目计划

iv. 通过权衡调整计划

v. 管理开发挑战

b. 建立一个工作分解结构

i. 分而治之，不然多数项目太大太复杂

ii. 工作分解结构（WBS):完成项目所需的任务层次结构

iii. 评估时间和成本

c. 建立一个项目计划

i. 甘特图

ii. 关键路径

d. 通过权衡调整计划

e. 管理开发过程中遇到的挑战

i. WBS基线

ii. 配置控制：系统开发人员用以维护对项目资源的控制的一组管理政策、实践和工具

6. scrum如何克服系统开发生命周期的问题
    a. 问题
        i. SDLC的本质否定了每位有经验的开发人员都知道的真实情况：系统需求含糊、变化——》却采用瀑布法（p426）
        ii. 具有风险
    b. scrum（敏捷开发方法）
        i. 开发规则（p428）
    c. scrum过程
        i. 基本要素
        ii. 什么时候结束
    d. 需求如何推动scrum过程
        i. 创建需求任务
        ii. 安排任务进度
        iii. 承诺完成任务
        iv. 哄骗?
7. 2027
    a. Fetch应用程序
    b. 用户驱动的系统
    c. 行业推动变革