第十章 物理安全需求

10.1 应用安全原则到选址和设施设计

10.1.1 安全设施计划

- 安全设施计划描述了组织的安全要求的轮廓，并且着重强调为了提供安全性所用的方法和机制
- 关键路径分析是一种系统工作，可以确定关键任务应用、过程和操作以及所有必要的支持要素之间的关系
- 检查关键路径时，已完成的评估或潜在的技术融合是很重要的，技术融合是不同的技术、解决方法、工具和系统在随着时间的推移进行发展和合并的趋势
- 安保人员应参与场所和设施的设计考虑

10.1.2 场所选择

- 场所的选择以组织的安全需要为基础，解决安全要求始终放在首位，自然灾害威胁，毗邻建筑物和业务、能够组织和防御明显的非法闯入企图很重要

10.1.3 可视性、可见性

- 可视性很重要，周围地形、设施、当地犯罪率

10.1.4 自然灾害

- 地区的自然灾害也是需要关注的方面

10.1.5 设施的设计

- 在进行设施的设计时，需要理解组织所需的安全等级，并计划和设计恰当的安全等级

10.2 设计和实施物理安全

- 物理安全管理控制分为三组：行政性的、技术性的和物理性的
- 行政性的包括设施构造和选择、场地管理、人员控制、意识培训和紧急事件响应及规程
- 技术性的包括访问控制、入侵检测、报警、闭路电视、监控、报文、通风、空调、电源以及火灾检查和排除
- 物理性的包括围栏、照明、锁、建筑材料、陷阱、狗和警卫
- 设计物理安全的控制措施顺序： 阻拦、拒绝、检测、延缓

10.2.1 设备故障

- 任务不紧急，48小时内替换
- 对老化的设备进行替换或维修应制定时间表

10.2.2 配线间

- 配线间的安全非常重要，重点在于防止未授权的物理访问方面

10.2.3 服务器机房

- 服务器机房应设在建筑物的核心位置

10.2.4 介质存储设施

- 介质存储设施应该被设计用于安全的保存空白介质、可重用介质和安全介质
- 可重用介质、应该被保护以防止被盗和残留数据恢复
- 安装介质要防止偷窃和恶意软件植入

10.2.5 证据存储

- 证据存储证迅速成为所有企业的必备品

10.2.6 受限的和工作区域安全

- 墙壁或隔离物都可以被用于隔开累死但不同的工作区域
- 每个工作站都 应当进行评估，并且像IT资产分类一样分门别类
- 设施安全设计过程应该支持内部安全的实施和维护

10.2.7 数据中心安全

- 智能卡：信用卡大小的身份证、员工证或通行卡，是一种完整的安全解决方法
  - 智能卡缺陷：容易遭受物理攻击、逻辑攻击、特洛伊木马攻击以及社会工程学攻击，智能卡一般为多因子认证
  - 记忆卡：具有磁条的、计算机可读的ID卡，记忆卡常作为一种双因子控制措施，记忆卡易于拷贝或复制
- 接近式读卡机：持卡人通过接近式读卡机时，接近式读卡机能够确定持卡人的身份以及是否被授权进行访问
  - 无线射频识别或生物测定学方面的访问控制设备来管理物理访问
- 入侵检测系统
  - 自动化的或人工的系统，用于检测未授权的个人企图发起的入侵、破坏和攻击行为
  - 物理入侵检测系统被称为防盗报警器，用于检测未经授权的活动并通知管理机构

    - 入侵检测失效的两方面：系统断电，如果断电可能不会功能做；系统通信线路被截断
- 访问滥用
    - 为了阻止滥用、尾随和伪装，必须部署保安人员或其他监控系统
    - 即使针对物理访问控制，审计跟踪和访问日志也仍然是非常有用的工具
- 放射防护
    - 阻止放射攻击的对策和防护类型被称为损失电磁脉冲设备屏蔽技术(TEMPEST)
    - TEMPEST的一些对策有法拉第笼、白噪声和控制区
    - 法拉第笼：完全包围区域所有面的金属网，金属网能够产生电容效应，防止电磁信号逸出
    - 白噪音：一直广播虚假通信数据，从而掩盖和隐藏实际的放射信号
    - 控制区：手续设备使用和支持放射信号的区域

10.2.8 基础设施和HVAC注意事项

不间断电源供应（UPS）可以为敏感的设备提供连续和平稳的电力
使用带有电涌保护器的配色盘，保护电源波动而遭受损坏
维持长时间的电力，需要一台发电机

- 电源术语
    - 故障（fault） 电力瞬间消失
    - 中断（balckout ）电力完全消失
    - 电压不足（sag） 瞬间电压降低
    - 降压（brownout）长时间低电压
    - 脉冲（spike） 瞬间高电压
    - 电涌（surge）长时间高电压
    - 启动功率（inrush）电源开始的电涌同行与连接的电源有关
    - 噪声（noise） 持续不断的电源干扰
    - 瞬时现象（transient）短时间的线路杂音干扰
    - 平稳（clean） 完全平稳的电流
    - 接地（groud）电路中的电线是接地的
- 噪声
  影响设备的功能，可能会干扰通信、传输和播放质量，电磁干扰分两种类型
    - 普通模式：电源或运转的电子设备的火线和地线的电势差产生
    - 导线模式：电源或运转的电子设备的火线和中线电势差产生
    - 保护设备不受噪声干扰的步骤：提供充足的电力条件、合适的接地措施、屏蔽素有电缆、以及限制暴露在EMI和RFI电源中
- 温度、湿度和静电
  温度保持在华氏60到75度之间、湿度维持在40%-60%之间，太高会侵蚀，太低会产生静电

表 10.1 静电电压及可能造成的损坏

静电电压(伏特)	可能造成的损坏
40	造成敏感电路和其他电子元件的损坏
1000	造成显示器显示时的不规则闪动
1500	造成硬盘上所存储数据的损坏
2000	突然性系统关闭
4000	打印机故障或元件损坏
17 000	永久性电路损坏

10.2.9 水的问题

- 如可能，防止服务器的房间和重要设备原理任何水源和传输管道
- 关键任务系统的地板周围安装水检测电路

10.2.10 火灾的预防、检测和抑制

- 灭火器：灭火器只有在或是刚刚开始时才起作用

表 10.2 灭火器分类

级别	火灾类型	灭火材料
A	普通的易燃品	水、苏打酸(干粉或液态化学物质)
B	液体	二氧化碳、哈龙*、苏打酸
C	电子	二氧化碳、哈龙*
D	金属	干粉

* 哈龙或 EPA 批准的哈龙替代物

- 防火检测系统 为了适当的保护设施免遭火灾，要求安装自动化检测和抑制系统
- 放水灭火系统
  - 湿管管道系统（封闭头系统）总是充满水，灭火装置出发就立刻放水
  - 干管道系统：包含压缩的控制，灭火装置被出发，控血泄露，打开水阀，管道中充满水并放出来
  - 洪水系统： 较粗的管道，大股的水流
  - 预先响应系统是干管道/湿管道系统的组合，适合计算机和人都存在的洒水系统
- 气体释放系统
  - 气体释放系统通常比放水系统有效，对人非常危险
- 损失
  - 烟对大多数存储设备有损坏
  - 热会损坏所有的电子和计算机组件
  - 灭火一直介质可能造成电路短路、加快侵蚀或导致设备无法使用

10.3 实施和管理物理安全

- 每个区域都有唯一且集中的物理访问控制、监控和预防机制

10.3.1 周边（访问控制和监控）

- 栅栏、大门、旋转门、陷阱
  - 栅栏是外围设备
    - 3到4英尺高的栅栏可以阻挡偶然的侵犯
    - 6到7英尺的栅栏可以组织大多数入侵者
    - 带3股铁丝网8英尺以上的栅栏可以阻挡信心坚定的入侵者
  - 大门是栅栏上收到控制的出入点
  - 陷阱通常是由保安人员守护的双重门设置，陷阱包括组织跟随者捎带和尾随的措施
- 照明
  - 关键区域应该2烛光英尺元、8英尺（1英尺=0.3米）高的地方被照亮
  - 照明主要目的是拦截偶然的入侵者、闯入者、小偷和希望在黑暗中实施恶意行为的潜在窃贼
- 保安和看门狗
  - 所有的物理安全控制最终都要依靠人的接入来阻止实际的入侵和攻击
  - 保安的缺点：受伤、生病、容易被迷惑、遭受社会工程学攻击、滥用资源

10.3.2 内部安全

- 钥匙和密码锁
  - 可编程的锁配置多种有效的访问号码
  - 锁可以作为边界进出的访问控制设备，也可以验证设备对进出授权和限制
- 员工证
  - 员工证、身份证或安全ID都是物理身份标识和/或电子访问控制设备的形式
  - 员工证可能被用于物理访问主要受到保安控制的环境中，还可以在扫描设备守卫而非保安守卫的环境中
- 活动探测仪
  运动探测仪或运动传感器是在特殊区域内使用的、用于感知物体运动的设备
  - 红外运动探测仪 对被监控区域红外照明模式的显著变化进行监控
  - 热能型运动探测仪 对被监控区域内的热能等级和模式的显著变化进行监控
  - 波形运动探测仪 向被监控的去发射连续的弱超声波或高频微博，并且对反射的波显著扰动或变化进行监视
  - 电容运动探测仪 对被监控物体周围区域的电场或磁场变化进行探测
  - 光电运动探测仪 在没有窗户或保持湖南的房间内部使用
  - 无源电频运动探测仪 对监视区域内的非正常声音进行侦听
- 入侵报警
- 环境出现重大或有意义的变化就会报警，报警分类一下几种
  - 威慑报警： 引发报警可能会采用额外的加锁，关门等措施，使得入侵或攻击变难

    - 排斥报警： 引发报警声通常听起来像汽笛或钟声，灯打开，另入侵者放弃攻击离开设施
    - 通知报警： 对于入侵者是缄默的，会记录相关数据，通知管理员、保安和执法机构
    - 本地报警：必须广播可听到的报警信号，必须受到保护，通常由保安进行保护，以防止损害好损失
    - 集中式报警系统：报警出发通过信号通告通知或集中式监控站，一般是有名的公司和国家安全公司
    - 辅助报警系统： 可以加入本地或者集中式报警，当安全边界破坏，通知紧急服务机构（消防、警察和医疗服务）做出响应
- 二次验证机制
  二次验证机制为了显著减少错误报警，并提高报警显示实际入侵或攻击的可能性
- 环境和生命安全
  保护环境的基本要素和保护人员生命是设施内物理访问控制和安全维护的重要方面，防止人员遭受生命书上是最重要的部分
- 隐私责任和法律需求
    - 隐私以为着保护个人信息不被泄露给未经任何授权的个人或实体
    - 对于任何组织，隐私保护应该是安全策略中 一个核心人物或目标
- 合规要求
  遵守所有的法律规定是维护安全的一个关键部分