第3章 物理安全

主要内容

3.1 概述

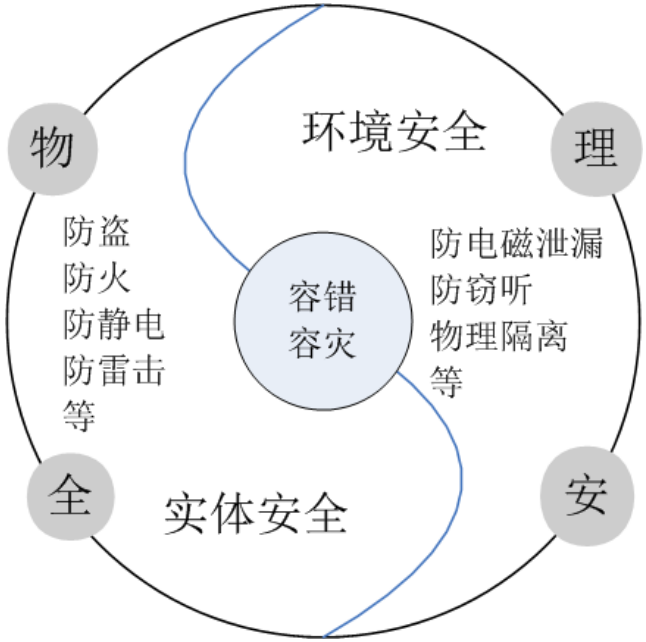
3.2 设备安全防护

3.3 防信息泄露

3.4 物理隔离

3.5 容错与容灾

3.1 概述



- 物理安全:实体安全和环境安全
- 解决两个方面问题:
  - 对信息系统实体的保护;
  - 对可能造成信息泄漏的物理问题进行防范。
- 物理安全技术包括:
  - 防盗、防火、防静电、防雷击、防信息泄漏、物理隔离;
  - 基于物理环境的容灾技术和物理隔离技术也属于物理安全技术范畴。
- 物理安全是信息安全的必要前提
  - 如果不能保证信息系统的物理安全，其他一切安全内容均没有意义。

3.2 设备安全防护

3.2.1 防盗

- 计算机也是偷窃者的目标，计算机偷窃行为所造成的损失可能远远超过计算机本身的价值，
- （1）安全保护设备
  - 有源红外报警器、无源红外报警器和微波报警器等；
  - 计算机系统是否安装报警系统，安装什么样的报警系统，要根据系统的安全等级及计算机中心信息与设备的重要性来确定。
- （2）防盗技术
  - 在计算机系统和外部设备上加无法去除的标识；
  - 使用一种防盗接线板，一旦有人拔电源插头，就会报警；
  - 可以利用火灾报警系统，增加防盗报警功能；
  - 利用闭路电视系统对计算机中心的各部位进行监视保护等。

3.2.2 防火

- 火灾因素：
  - 电气原因、人为因素或外部火灾蔓延引起的
- 计算机机房的主要防火措施如下：
  - 计算机中心选址
  - 建筑物的耐火等级
  - 不间断供电系统或自备供电系统
  - 防雷设施与抗静电地板
  - 严禁存放腐蚀性物品和易燃易爆物品
  - 禁止吸烟和随意动火

3.2.3 防静电

- 静电产生：接触→电荷→转移→偶电层形成→电荷分离。
- 静电是一种电能，具有高电位、低电量、小电流和作用时间短的特点。
- 静电放电火花造成火灾，还能使大规模集成电损坏，这种损坏可能是不知不觉造成的。
- 静电防范：
  - 静电的泄漏和耗散、静电中和、静电屏蔽与接地、增湿等。防范静电的基本原则是“抑制或减少静电荷的产生，严格控制静电源”。

3.2.4 防雷击

- 雷电防范的主要措施是：
  - 根据电气及微电子设备的不同功能及不同受保护程序和所属保护层来确定防护要点做分类保护。
- 常见的防范措施主要包括：
  - 接闪
    - 让闪电能量按照人们设计的通道泄放到大地中去。
  - 接地
    - 让已经纳入防雷系统的闪电能量泄放入大地。
  - 分流
    - 一切从室外来的导线与接地线之间并联一种适当的避雷器，将闪电电流分流入地。
  - 屏蔽
    - 屏蔽就是用金属网、箔、壳、管等导体把需要保护的对象包围起来，阻隔闪电的脉冲电磁场从空间入侵的通道。

3.3 防信息泄露

3.3.1 电磁泄露

- 电磁干扰EMI（Electro Magnetic Interference）
  - 是指一切与有用信号无关的、不希望有的或对电器及电子设备产生不良影响的电磁发射。
- 防止EMI要从两个方面来考虑，
  - 减少电子设备的电磁发射；
  - 提高电子设备的电磁兼容性EMC。
- 电磁兼容性EMC（Electro Magnetic Compatibility）
  - 电子设备在自己正常工作时产生的电磁环境，与其它电子设备之间相互不影响的电磁特性。

TEMPEST

- TEMPEST技术（Transient Electromagnetic Pulse Emanation Standard）
  - 计算机信息泄漏安全防护技术，是一项综合性的技术，包括泄露信息的分析、预测、接收、识别、复原、防护、测试、安全评估等项技术，涉及到多个学科领域。
  - 通常我们把输入、输出的信息数据信号及它们的变换称为核心红信号。
  - 那些可以造成核心红信号泄密的控制信号称为关键红信号，红信号的传输通道或单元电路称为红区。
  - 所谓的“TEMPEST”要解决的问题就是防止红信号发生电磁信息泄漏。

防电磁信息泄漏

- 主要包括三个层面，
  - 一是抑制电磁发射，采取各种措施减小“红区”电路电磁发射；
  - 二是屏蔽隔离，在其周围利用各种屏蔽材料使红信号电磁发射场衰减到足够小，使其不易被接收，甚至接收不到；
  - 三是相关干扰，采取各种措施使相关电磁发射泄漏即使被接收到也无法识别。

常用的防电磁泄漏的方法

- 屏蔽法（即空域法）
  - 屏蔽法主要用来屏蔽辐射及干扰信号。采用各种屏蔽材料和结构，合理地将辐射电磁场与接收器隔离开，使辐射电磁场在到达接收器时强度降低到最低限度，从而达到控制辐射的目的。
  - 空域防护是对空间辐射电磁场控制的最有效和最基本的方法，机房屏蔽室就是这种方法的典型例子。

- 频域法
  - 频域法主要解决正常的电磁发射受干扰问题。不论是辐射电磁场，还是传导的干扰电压和电流都具有一定的频谱，即由一定的频率成分组成。
  - 通过频域控制的方法来抑制电磁干扰辐射的影响，即利用系统的频率特性将需要的频率成分(信号、电源的工作交流频率)加以接收，而将干扰的频率加以剔除。
  - 频域法就是利用要接收的信号与干扰所占有的频域不同，对频域进行控制。

- 时域法
  - 与频域法相似，时域法也是用来回避干扰信号。
  - 当干扰非常强，不易受抑制、但又在一定时间内阵发存在时，通常采用时间回避方法，即信号的传输在时间上避开干扰。

3.3.2 窃听

- 窃听是指通过非法的手段获取未经授权的信息。
- 窃听技术
  - 指窃听行动所使用的窃听设备和窃听方法的总称。
- 防窃听
  - 指搜索发现窃听装置及对原始信息进行特殊处理，以达到消除窃听行为或使窃听者无法获得特定原始信息。
- 防窃听技术
  - 检测主要指主动检查是否存在窃听器，可以采用电缆加压技术、电磁辐射检测技术以及激光探测技术等；
  - 防御主要是采用基于密码编码技术对原始信息进行加密处理，确保信息即使被截获也无法还原出原始信息，另外电磁信号屏蔽也属于窃听防御技术。

3.4 物理隔离

- **3.4.1 物理隔离的理解**
  - 较早时描述的单词Physical Disconnection
  - 后来Physical Separation和Physical Isolation
  - 目前开始使用Physical Gap这个词汇，直译为物理隔离，意为通过制造物理的豁口，来达到物理隔离的目的。

对物理隔离的理解表现:

（1）阻断网络的直接连接

（2）阻断网络的Internet逻辑连接

（3）隔离设备的传输机制具有不可编程的特性

（4）任何数据都是通过两级移动代理的方式来完成，两级移动代理之间是物理隔离的。

（5）隔离设备具有审查的功能。

（6）隔离设备传输的原始数据，不具有攻击或对网络安全有害的特性

（7）强大的管理和控制功能。

（8）从隔离的内容看，隔离分为网络隔离和数据隔离。

3.4.2物理隔离与逻辑隔离

- 物理隔离与逻辑隔离有很大的区别，
  - 物理隔离的哲学是不安全就不连网,要绝对保证安全；
    - 物理隔离部件的安全功能应保证被隔离的计算机资源不能被访问（至少应包括硬盘、软盘和光盘），计算机数据不能被重用（至少应包括内存）。
  - 逻辑隔离的哲学是在保证网络正常使用下,尽可能安全
    - 逻辑隔离部件的安全功能应保证被隔离的计算机资源不能被访问，只能进行隔离器内外的原始应用数据交换。

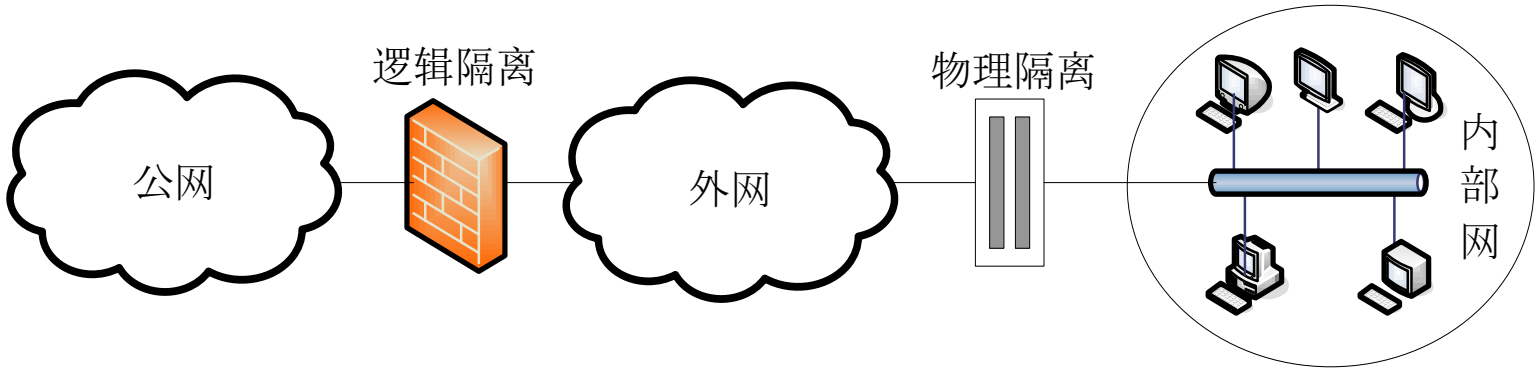


图3.2 企业网络的划分

3.4.3 网络物理隔离的基本形式

① 内外网络无连接，内网与外网之间任何时刻均不存在连接，是最安全的物理隔离形式。

② 客户端物理隔离，采用隔离卡使一台计算机既连接内网又连接外网，可以在不同网络上分时地工作，在保证内外网络隔离的同时节省资源、方便工作。

③ 网络设备端物理隔离，在网络设备处的物理隔离常常要与客户端的物理隔离相结合，它可以使客户端通过一条网线由远端切换器连接双网，实现一台工作站连接两个网络的目的。

④ 服务器端物理隔离，实现在服务器端的数据过滤和传输，使内外网之间同一时刻没有连线，能快速、分时地传递数据。

3.5 容错与容灾

3.5.1 容错

- 保证系统可靠性的三条途径
  - 避错是完善设计和制造，试图构造一个不会发生故障的系统，但这是不太现实的
  - 纠错做为避错的补充。一旦出现故障，可以通过检测、排除等方法来消除故障，再进行系统的恢复。
  - 容错是第三条途径。其基本思想是即使出现了错误，系统也可以执行一组规定的程序；

容错系统

① 高可用度系统：可用度用系统在某时刻可以运行的概率衡量。高可用度系统面向通用计算机系统，用于执行各种无法预测的用户程序，主要面向商业市场。

② 长寿命系统：长寿命系统在其生命期中不能进行人工维修，常用于航天系统。

③ 延迟维修系统：延迟维修系统也是一种容灾系统，用于航天、航空等领域，要求满足在一定阶段内不进行维修仍可保持运行。

④ 高性能系统：高性能系统对于故障（瞬间或永久）都非常敏感，因此应当具有瞬间故障的自动恢复能力，并且增加平均无故障时间。

⑤ 关键任务系统：关键任务系统出错可能危及人的生命或造成重大经济损失，要求处理正确无误，而且恢复故障时间要最短。

常用的数据容错技术

① 空闲设备：也称双件热备，就是备份两套相同的部件。当正常运行的部件出现故障时，原来空闲的一台立即替补。

② 镜像：镜像是把一份工作交给两个相同的部件同时执行，这样在一个部件出现故障时，另一个部件继续工作。

③ 复现：复现也称延迟镜像，与镜像一样需要两个系统，但是它把一个系统称为原系统，另一个成为辅助系统。辅助系统从原系统中接收数据，与原系统中的数据相比，辅助系统接收数据存在着一定延迟。

④ 负载均衡：负载均衡是指将一个任务分解成多个子任务，分配给不同的服务器执行，通过减少每个部件的工作量，增加系统的稳定性。

3.5.2 容灾

- 容灾的含义是对偶然事故的预防和恢复。
- 解决方案有两类
  - 对服务的维护和恢复；
  - 保护或恢复丢失的、被破坏的或被删除的信息。
- 灾难恢复策略
  （1）做最坏的打算
  （2）充分利用现有资源
  （3）既重视灾后恢复，也注意灾前措施
- 数据和系统的备份和还原
  - 是事故恢复能力的重要组成，
  - 数据备份越新、系统备份越完整的机构部门就越容易实现灾难恢复操作。

Any question?