第五章 保护资产的安全

5.1 对资产进行分类和标记

5.1.1 定义敏感数据

- 敏感数据指所有不公开或未分类的数据
  i. 个人信息身份
  ii. 受保护的健康信息
  iii. 专有数据：任何帮助组织保持竞争优势的数据

5.1.2 定义分类

- 政府数据分类为绝密、保密、机密和非机密
- 非政府分类 机密或专业、私有、敏感、公开

5.1.3 定义数据安全要求

表 5.1 保护电子邮件数据安全

分类	对电子邮件的安全需求
机密	电子邮件和附件必须用 AES 256 加密 电子邮件和附件除了被浏览时要一直保持被加密 电子邮件只能在组织内发送给收件人 电子邮件只能被收件人打开和浏览(被发送邮件不能被打开) 附件能被打开和浏览，但不能保存 电子邮件的内容不能被拷贝和粘贴到其他文档中 电子邮件不能被打印
隐私	电子邮件和附件必须用 AES 256 加密 电子邮件和附件除了被浏览时要一直保持被加密 电子邮件只能在组织内发送给收件人
敏感	电子邮件和附件必须用 AES 256 加密
公开	电子邮件和附件能够以明文形式发送

5.1.4 理解数据状态

- 静态数据：存储在介质上的数据
- 传输数据：通过网络传送的数据
- 使用的数据：临时存储区中正在被应用程序使用的数据
- 保护数据最好的办法就是使用强大的加密协议，此外身份认证、授权控制能有效防止未经授权的访问

5.1.5 管理敏感数据

管理敏感数据的主要目标就是防止数据泄露

1. 标记敏感数据：敏感数据进行标记能够确保用户能够轻松识别任何数据的分类级别，标记氛围物理标签、数字水印或标签、标题、脚注
2. 管理敏感数据：介质的整个生命周期内确保传送过程的安全
    - 备份磁带应该与备份数据一样受到同级别保护
3. 存储敏感数据：
    - 敏感数据应存储在受保护且没有任何损失的介质中，最有效的保护办法就是加密
    - 遵循基本的物理安全做法，如防止偷窃
    - 采取环境控制来保护介质的数据安全，如湿度和温度控制
    - 任何敏感数据的价值都大于存储介质的价值
4. 销毁敏感数据
    - 数据剩磁：数据仍然作为剩余磁道上的数据保留在硬盘驱动器上
    - 消磁工具：删除数据剩磁的一种方法，但该方法仅对磁介质有效
        - 最好的净化方法是销毁固态硬盘
    - 销毁数据常见术语
        a. 擦除：介质上的数据就是对文件、文件的选择或整个介质执行删除操作，可以被复原
        b. 消除：介质重写的过程，确保消除的数据不会通过传统的工具恢复，可通过高级工具获取原始数据
        c. 清除：比消除更强烈的形式，将消除过程多次重复并结合其他方法，但并不总是可靠
        d. 解除分类：在非机密情况下对介质或系统进行清除，以便其能够再次使用的准备过程
        e. 净化：从系统或介质中删除数据，确保数据不会以任何形式恢复
        f. 销毁：介质生命周期的最后阶段，也是最安全的方法
5. 保留资产 保留要求适用与数据或者记录、含有敏感数据的介质和系统，以及接触敏感数据的人员

5.1.6 应用密码学保护机密文件

1. 应用对称加密保护数据
    - 高级加密标准算法(AES)：
    - 三重数据加密标准算法(3DES)
    - Blowfish：可作为数据加密标准的可选择项
2. 应用传输加密保护数据
    - 传输加密在传播之前加密数据，对传输过程中的数据进行保护
    - 网络浏览器使用HTTPS来加密电子商务交易，使用TLS作为基本加密协议
    - 远程访问使用VPN，VPN使用TLS+ IPSec或者L2TP+IPSec

- IPSec包括一个认证报头(AH),该认证报头提供鉴定和完整性，封装安全载荷(ESP)提供保密性

5.2 定义数据角色

5.2.1 数据所有者

- 数据的最终负责人，通常为首席执行官、总裁或部门主管

5.2.2 系统所有者

- 拥有含机密数据的系统的人
- 系统所有者负责确保系统中运行的数据的安全性

5.2.3 业务/任务所有者

- 拥有流程，并确保系统对组织的价值，一般为项目经理或信息系统所有者

5.2.4 数据处理者

- 通常为组织处理数据的第三方实体

5.2.5 管理员

- 基于数据所有者提供的指导方针授权访问数据

5.2.6 保管者

保管者通过以适当的方式保存和保护数据，协助保护数据的安全性和完整性

5.2.7 用户

任何通过计算机系统获取数据并完成工作的人

5.3 保护隐私

1. 使用安全基线：
   - 安全基线确保最低安全标准，审计程序须周期性的检查系统，以去报维持在安全状态
2. 审视和定制
   - 审视： 评估基线安全控制，然后只选择那些适用于想保护的IT系统的控制
   - 定制： 修改基线内的安全控制列表，使其与组织的使命相适应
3. 选择标准
   - 选择基线内的安全控制时，组织需要确保控制符合某些外部安全标准