第十六章 管理安全运营

16.1 应用安全运营概念

- 安全运营实践的主要目的是保障系统中信息资产的安全性

16.1.1 知其所需和最小特权

- 知其所需和最小特权是值得在任何IT安全环境中采纳的两条标准原则
  - 知其所需访问：利用需求来给用户授权，仅根据为完成所分配任务而授权访问需要操作的数据或资源，目的是为了保持机密性
  - 最小特权
    - 表明主体仅仅授予执行已分配工作任务的特权，不会拥有超出其工作任务的特权，目的是保护完整性
    - 最小特权原则不仅仅延伸到数据访问，也应用到系统访问中
- 其他的人员概念：
  - 授予：授予特权设计一系列用户获取的特权
  - 聚合：最小特权环境下的聚合设计用户随着时间而收集到的一系列特权
  - 传递信任：非信任传递出现在两个安全域中，信任传递扩展了两个安全域以及他们的所有子域之间的信任关系

16.1.2 职责和责任分离

- 职责和责任分离确保没有单个人能控制某个关键功能和整个系统，确保没有单个人能危害到系统或系统的安全性
- 职责分离策略建立了一个相互支援和平衡的系统
  - 特权分离
    - 特权分离类似于任务和职责分离的概念，建立在最小特权原则上并应用到应用程序和进程中，特权分离策略要求使用颗粒状的权限和许可
  - 职责划分
    - 职责划分类似于任务和责任分离的策略，但也结合最小特权原则，目的是确保个人没有可能导致成立以冲突的额外系统访问
  - 双人控制
    - 类似于职责划分，需要两个人认同关键任务，确保了并行互审，减少共谋和欺骗的可能性

16.1.3 岗位轮换

- 岗位轮换作为安全控制可以提供并行审查，减少欺骗并促进交叉培训

16.1.4 强制休假

- 提供一种互审形式，有助于检测欺诈和共谋

16.1.5 监控特殊的权限

- 特殊的权限操作是一项需要特殊访问或较高的权限来执行许多管理员和敏感工作任务的活动
- 通常任何类型的管理员账户都有高级特权并应该监控他，也能授予用户较高的特权但不给用户授予所有的管理访问权

16.1.6 管理信息生命周期

- 安全控制保护了整个生命周期内的信息，通用方法包括标记、处理、存储和恰当销毁数据
  - 标记数据：确保用户能很容易的标识数据价值，用户应该在创建数据后不久就标记他们
  - 处理数据：主要涉及数据的传输，并且关键是在传输过程中提供与数据存储相同级别的保护
  - 存储数据：数据存储的位置需要得到保护一起防止丢失，数据主要存储在磁盘驱动上，需要人周期性的备份有价值的数据
  - 销毁数据：以一种数据不可读的方式来销毁

16.1.7 服务级别协议

- SLA（服务级别协议）是组织和外部实体之间的一份协定，保证对性能的期望被满足，不能满足这些期望会受到处罚

16.1.8 关注人员安全

- 关注人员安全是安全运营中非常重要的安全因素

16.2 提供和管理资源

- 安全运营知识域的另一个元素就是整个生命周期中的资产配置及管理

16.2.1 管理硬件和软件资产

- 硬件清单
  - 许多组织使用数据库和库存应用程序来清点库存和跟踪硬件资产
  - 无线射频识别（RFID）标签可以减少清点库存的时间
  - 保存敏感数据的编写介质设备也视为一种资源
- 软件许可

    - 组织购买软件，并经常使用许可证秘钥来激活软件，软件许可确保系统没有未授权的软件安装

16.2.2 保护物理资产

- 物理资产在IT硬件之外，包括所有的物理设施，如办公建筑以及内部设施，栅栏，路障，安保，闭路电视系统等

16.2.3 管理虚拟资产

- 为了大幅度节约成本，组织逐步使用越来越多的虚拟化技术，虚拟资产如下：
    - 虚拟机（VM）
    - 软件定义网络（SDN）:将控制平面从数据平面中分离出来
    - 虚拟存储区域网络（VSAN） 虚拟化的存储设备

16.2.4 管理基于云的资产

- 云的服务模式：
    - 软件即服务（SaaS）:通过web浏览器提供全功能的应用程序
    - 平台即服务（PaaS）：为消费者提供一个计算平台，包括硬件、操作系统和应用程序
    - 基础设施即服务（IaaS）:为消费者提供基本的计算资源，包括服务器，存储和某些情况下的网络资源，消费者自己安装操作系统和应用程序
- 云模式：
    - 公共云：任何消费者租用的资产由外部CSP管理
    - 私有云：组织自己的资源创建和管理私有云
    - 社区云：两个或多个组织提供云基础资产
    - 混合云： 两个或两个以上的云组合

16.2.5 介质管理

- 介质管理是采用措施管理保护介质和存储在介质上的数据
- 当介质包含敏感信息时，信息应该被存储在安全的位置，并且加以严格的访问控制
- 介质管理还可以包括使用技术控制来限制来自于计算机系统的设备访问
    - 磁带介质管理
        - 磁带常易因腐蚀而被破坏，最好保留两份备份
        - 存储区的清洁度将直接影响磁带介质设备的寿命和实用性
    - 移动设备
        - 移动设备包括智能手机和平板电脑

16.2.6 管理介质的生命周期

- 一旦备份介质已达到其寿命，就要进行销毁

16.3 配置管理

- 配置管理有助于保护系统处于一致安全的状态，并在整个生命周期维护这种状态

16.3.1 基线

- 当系统处于部署在有安全基线状态下时，系统会更安全
- 基线可与检查列表同事产生，脚本和操作系统工具被用来实现基线，使用自动的方法减少手动基线的潜在错误

16.3.2 用镜像创建基线

- 管理员在计算机上安装操作系统和所需的应用程序
- 管理员使用镜像制作软件捕获系统的镜像
- 手动将镜像部署到系统中

16.4 变更管理

- 变更管理有助于减少由于未授权变更造成的不可预料的中断，变更管理的目的是确保变更不会导致中断
- 变更可能会削弱安全性

16.4.1 安全影响分析

- 专家对变更管理进行评估并识别安全影响之后，工作人员才开始实施变更
- 变更的常见步骤：
  - 请求变更：工作人员请求变更
  - 审查变更：专家审查变更
  - 批准/拒绝变更：专家批准和拒绝变更
  - 计划和实施变更：
  - 记录变更：记录变更以确保所有相关人员熟悉变更

16.4.2 版本控制

- 版本控制指软件皮遏制管理中使用的版本控制，如果不能通过某种类型的版本控制系统来控制变更，可能会引发变更导致的网站瘫痪

16.4.3 配置文档

- 配置文档确定当前系统的配置，定义系统负责人和系统目标，应用于基线的变更

16.5 补丁管理和减少漏洞

- 补丁管理和漏洞管理同时用于保护企业的系统免受威胁

16.5.1 补丁管理

- 补丁是用于任何类型代码编写的笼统术语
- 补丁管理的共同步骤
  - 评估补丁： 供应商发布补丁后，管理员评估补丁，已确定补丁适用于他们的系统
  - 测试补丁： 管理员随时测试单一系统的补丁，以确定补丁不会带来其他副作用
  - 批准补丁：测试补丁并确定安全性之后，批准补丁
  - 部署补丁：经过测试和皮核准，管理员部署补丁
  - 确认补丁已部署：部署补丁后，管理员定期测试和审计系统，以确保系统补丁仍然有效

16.5.2 漏洞管理

- 漏洞管理是指定期检测漏洞，评估并采取相应措施来减少相关风险，漏洞管理程序的常见要素是漏洞扫描和定期脆弱性评估

16.5.3 漏洞扫描

- 漏洞扫描是用来测试系统和网络有无已知安全问题的软件工具，攻击者利用漏洞扫描检测系统和网络中的漏洞

16.5.4 漏洞评估

- 漏洞评估通常包含漏洞扫描结果，漏洞扫描评估往往是风险分析和风险评估的一部分

16.5.5 常见漏洞和披露

通用漏洞披露（CVE）列表，CVE数据库为组织创建补丁管理和漏洞管理提供了方便