第十七章 事件预防和响应

17.1 管理事件响应

- 任何安全程序的主要目标之一就是防止安全事件发生

17.1.1 事件界定

- 事件时对组织资产的保密性、完整性和可用性有负面影响的事故
- 计算机安全事件通常是指攻击接口，或指部分用户来说是恶意或故意行动的结果

17.1.2 事件响应步骤

- 有效的时间响应氛围几个步骤或处理阶段
- **检测、响应、缓解、报告、恢复、修复、经验教训**

17.1.3 检测

- IT环境包括许多检测潜在时间的方法，常用的有：
  - 相匹配的事项发生时，入侵检测和防御系统发送告警给管理员
  - 检测到恶意软件时，反恶意软件会显示弹出窗口加以提示
  - 许多自动化工具定期扫描审计日志，寻找预定义的时间
  - 最终用户有时会发现不规则的活动，并联系技术人员或者管理员寻求帮助

17.1.4 响应

- 检测和验证时间后，下一步就是响应，响应程度取决于事件的严重程度
- 团队成员应该对时间响应好组织的时间响应计划进行培训
- 组织如果能较快的响应一个时间，就可以更好的机会减少损害
- 在调查结束后，管理层可能决定起诉责任人，因此调查过程中保护所有的数据作为证据

17.1.5 缓解

- 缓解措施尝试遏制事件，有效的事件响应的主要目标之一是限制事件的影响范围

17.1.6 报告

- 报告是指组织内部并同时向组织外部报告事件，针对严重的安全事故，组织应考虑到报告事件给官方机构

17.1.7 恢复

- 调查人员从系统收集所有适当的证据后，下一步就是恢复系统或将系统恢复到完全正常的状态
- 当受损的系统重建时，重要的是确保配置正确

17.1.8 修复

- 在修复阶段，人员观察事件并确定什么原因导致事件发生，然后措施以防止再次发生
- 执行根本原因分析的目的是为了确定什么原因导致事件发生

17.1.9 经验教训

- 在检测事件响应时，人们可以寻找改进响应的任何方面，完成经验审查后，通常需要事件响应团队编写一份报告

17.2 部署预防措施

- 组织可以通过实时预防措避免事故

17.2.1 基本的预防措施

- 一些对能抵抗大多数典型攻击措施有帮助的步骤：
  - 保持系统和应用程序最新：补丁管理能确保系统和应用程序上安装最新的相关补丁
  - 删除和禁用不必要的服务和协议：缩小被攻击的面
  - 使用入侵检测和防御系统： 试图检测攻击，并提供报警
  - 使用最新的反恶意软件：涵盖各种类型的恶意代码
  - 使用防火墙： 防火墙可以阻挡许多不同类型的攻击

17.2.2 理解攻击

- 常见的攻击
  - 拒绝服务攻击： 能够阻止系统处理或响应来自资源和客体的合法数据和请求，拒绝服务攻击会导致系统崩溃、系统重启、数据损坏、服务被阻断等
    - SYN泛洪攻击：通过破坏TCP/IP启动通信会话的三步握手标准来实施攻击
  - smurf和fraggle攻击
    - smurf和fraggle属于dos攻击
    - smurf是一种泛洪攻击，使用受害者的IP地址作为源IP地址伪造广播Ping
    - fraggle攻击类似于smurf，使用UDP端口7和19，伪造IP地址发送UDP数据包发送给受害者
  - ping泛洪攻击
    - ping泛洪攻击通过给受害者发送洪水般的请求来达到攻击目的

- 僵尸网络
  - 僵尸网络中的计算机，将会按照攻击者要求的命令执行，发起大范围攻击，发送垃圾邮件和钓鱼邮件
- 死亡ping
  - 采用一个超大的ping数据包，现在死亡ping攻击很少成功
- 泪滴攻击
  - 攻击者阻碍传输，系统无法将数据包一起发送，泪滴攻击以一种系统无法将文件还原的方式分割数据包，目前系统部容易受到泪滴攻击
- land攻击
  - 攻击者使用受害者的IP地址作为源地址和目的地址，发送伪造的SYN数据包给受害者，自己不断的做出回应，并最终可能会冻结、崩溃和重新启动
- 零日攻击
  - 利用他人未知的系统漏洞对系统发现攻击
  - 保护零日漏洞攻击的方法包括许多基本预防措施，不运行不需要的服务和协议，使用基于网络和基于主机的防火墙，使用入侵检测和防御系统检测和组织潜在攻击，使用蜜罐和填充单元
- 恶意代码
  - 在计算机系统上执行不必要、未授权的或位置活动的脚本或者程序
  - 偷渡式下载可以未经用户许可就将恶意软件下载并安装到用户的系统
  - 安装恶意软件的另一种流行方法就是使用付费的安装方法
- 中间人攻击
  - 当恶意用户能够逻辑上获得正在进行通信的两个端点之间的位置时，中间人攻击就会产生
  - 通过保持系统最新补丁，能够预防一些中间人攻击，入侵检测系统能检测通信线路上的异常活动
- 战争拨号
  - 一种使用调制解调器搜素接受入栈连接尝试的系统的行为
  - 新的战争拨号能够在不使用调制解调器的情况下，使用互联网协议拨号
  - 抵御战争拨号的对策包括：实施强大的远程访问安全，确保不存在未授权的调制解调器，使用回叫安全机制，协议约束和呼叫登入
- 破坏
  - 破坏指的是员工对组织的破坏行为
  - 预防破坏的措施：禁用解雇员工账号，定期审计，检测异常和未授权的活动
- 间谍
  - 一种收集专有的、秘密的、私人的、敏感或机密信息的恶意行为
  - 严格控制访问所有的非公开数据，彻底筛查新的员工，并有效跟踪员工活动

17.2.3入侵检测和防御系统

- 入侵检测是一种特定形式的检测，通过监控记录信息和实时事件来检测潜在时间或入侵的异常活动

- 入侵防御系统有入侵检测的所有功能，还可以采取额外的措施来组织或防止入侵
- 基于知识和基于行为的检测
  - 基于知识的入侵检测（匹配模式检测或基于签名的检测）：使用入侵检测系统供应商开发的数据库，缺点是仅对已知的攻击方法有效
  - 基于行为的入侵检测（统计入侵检测、异常入侵检测、基于启发式的检测）：基于检测最开始在系统中创建正常获得和时间的基线，基于行为的入侵检测可以被认为是专家系统和伪人工系统，缺点是会发现大量的假报警
- IDS响应
  - 被动响应： 系统通过电子邮件、文本、寻呼消息或弹出消息的方式将信息发送给管理员
  - 主动响应：使用集中不同的方法来修改环境，典型ed如通过修改ACL组织基于端口、协议和源地址的流量输出
- 主机性和网络型IDC
  - IDC根据信息来源分类
    - 主机型IDS：监控单个计算机上的活动，可以检测到主机系统上的异常，缺点是费用和相关的可用性，降低主机的性能
    - 网络型IDS：检测并评估网络活动来检测攻击事件或异常，不能检测加密流量的内容，可以检测其他数据的信息
      - 优点：整体性能的负面影响较小
      - 缺点： 能检测攻击或将要进行的攻击，但是不能提供有关攻击成功的信息
- 入侵防御系统
  - 入侵防御系统（IPS）是一种特殊类型的主动入侵检测系统，能够在攻击达到目标系统之前检测并阻止，所有流量都必须经过IPS，IPS在分析后选择将流量通过或组织，IDS只有在攻击到达目标之后才能检测到，IPS可以使用基于知识或基于行为的检测
- 理解黑暗网络
  - 黑暗网络使用已分配的，不用IP地址网络ongoin空间的一部分，包括一台已配置为捕获所有进入黑暗网络的流量的设备

17.2.4 特殊的防御措施

- 蜜罐/蜜网：创建独立的及实际作为陷阱来捕获入侵者，目的使入侵者远离保留有机制资源的合法网络，同时在不破坏真实环境下观察攻击者的活动
- 理解伪漏洞：故意植入系统中，视图引诱攻击者的虚假漏洞或明显漏洞
- 理解填充单元：和蜜罐类似，但是使用不同的方式来隔离入侵，填充单元是模拟环境
- 警告框：将基本安全策略准则通知给用户和入侵者，提示他们在线活动会被审计和监控，并提供受限的活动提醒
- 反恶意软件：组织恶意代码最重要的措施就是带有最新签名的反恶意软件，
- 白名单和黑名单：可以有效组织用户运行未授权的 应用程序
- 防火墙：通过过滤流量为网络提供保护

    - 基本防火墙：使用协议号过滤基于IP地址、端口和一些协议的流量
    - 第二代防火墙：添加额外的过滤功能，应用级网关防火墙基于特定应用需求的流量，电路级防火墙过滤基于通信的流量
    - 第三代防火墙（状态监测防火墙和动态数据包监测防火墙）：基于状态的流量
    - 下一代防火墙：含有统一威胁管理装置的功能
- 沙箱：提供一个安全边界，组织应用程序与其他应用程序交互
- 第三方安全服务：一些组织奖安全服务外包给第三方
- 渗透测试：模仿实际攻击，尝试确定攻击者会使用哪些技术绕过应用程序、系统、网络和组织的安全性
    - 渗透测试风险： 有些操作可能导致中断
    - 获得渗透测试权限：经过高级管理人仔细深意和批准后才能进行渗透测试
    - 渗透测试技术：组织聘请外部顾问进行渗透测试很常见
    - 零知识团队黑盒测试
    - 全知识团队白盒测试
    - 部分知识会和测试
    - 防护报告： 渗透测试人员提供一份记录测试结果的报告，且该报告作为敏感信息而被保护
    - 道德黑客行为：了解网络安全知识并指导如何破解安全性，却不利用该知识为自己谋利的人

17.3 日志、监控和审计

17.3.1 日志和监控

1. 日志技术
    - 日志记录：将事件的信息记录到日志文件或数据库的过程
2. 通用日志类型：
    - 安全日志：记录一些对资源的访问
    - 系统日志：记录系统或服务的开启或关闭等事件
    - 应用程序日志：记录特定应用程序的信息
    - 防火墙日志： 记录与到达防火墙的流量相关的任何事件
    - 代理日志：记录详细的代理功能
    - 变更日志： 记录变更请求，批准和系统的实际变更
3. 保护日志数据
    - 中央系统上存储日志副本是很常见的保护日志方法
    - 对实施日志文件备份的组织有严格的管理策略
4. 角色监控
    - 监控功能为组织增加可问责性、帮助调查、提供基本的故障排除方法
        - 监控和可问责性

        - 监控能确保受监控着可以对他们的行为和活动负责
    - 监控和调查
        - 审计跟踪通使得调查人员在发生事件之后能够对其进行重建
    - 监控和问题识别
        - 监控跟踪为管理员提供一些有用的、与事件相关的详细信息
5. 监控技术
    - 监控是一种检查信息日志并寻找具体某些细节的过程
        - 日志分析是检测过程中一种详细且系统化的模式
        - 手动分析日志，管理员只需打开日志文件
        - 安全信息和事件管理
            - 许多组织使用集中式应用程序来自动监控网络上的系统
            - 安全信息和事件管理（SIEM）、安全事件管理（SEM）和安全信息管理（SIM）
        - 审计跟踪
            - 审计跟踪提供了系统活动的记录，并可以重建导致安全事件的活动
        - 抽样
            - 从大量的数据中提取元素的过程
        - 阀值级别
            - 它只选择超过阀值平均值的时间，阀值平均值是时间的预定义阀值
    - 其他监控工具
        - 击键监控： 记录用户在物理键盘上的记录行为
        - 流量分析和趋势分析：对数据包的流量进行检测

17.3.2 出口监控

出口监控是指检测传出去的流量、以防止数据泄露

1. 数据泄露保护（DLP）：能够检测和阻止数据邪路的企图
    - 基于网络的DLP：扫描所有网络输出数据以寻找具体的数据
    - 基于终端的DLP：可以扫描存储在系统中的文件以及发送到外部设备的文件
    - DLP通常具备进入深层次检查的能力
2. 隐写术
    - 隐写术指的是在文件中嵌入消息
3. 水印
    - 水印指的是在纸上嵌入不容易感知的图像或图案，经常用来防止伪造货币

17.3.4 审计和评估有效性

审计是对环境有条理的进行检查和审查，目的是确保符合法规，还能检测异常、未授权的事件或犯罪

审计人员负责测试和验证安全策略或法规的具体落实过程和程序

1. 检验审计：来发现和纠正漏洞
2. 访问审计：检测用户权限，以及确保安全流程和程序都正常运行
3. 用户权限审计： 在用户权限的背景下，最小特权
4. 特权组审计：限制小组成员只有在必须时才使用它们的搞特权账户
5. 高级别管理组：
6. 双重管理员账号：管理员拥有两个账号，一个日常使用，一个账号额外特权
7. 安全审计和审查：帮助组织确定正确实施安全控制，审查条目有
    - 补丁管理
    - 漏洞管理
    - 配置管理
    - 变更管理
8. 报告审计结果
9. 保护审计结果：审计报告包含敏感信息，只有足够特权的人能够访问审计报告
10. 发布审计报告
11. 使用外部审计师