分析一个典型的windows10-x86主机安全体系结构

2151140 王谦

> - SEC1 用OSI7层和tcp/ip4层模型分解或划分其系统组件或软硬件结构
> - SEC2 简要概括其实现cia的安全策略和安全机制，一一对应到基本组件
> - 典型的windows10-x86笔记本主机:windows10+sql+office

SEC1: 使用OSI七层模型和TCP/IP四层模型分解主机的系统组件和软硬件结构

OSI七层模型分解

1. **物理层（Physical Layer）**
   - **硬件设备**：
     - **计算机硬件**：CPU、内存、硬盘、主板、显示器、键盘、鼠标等。
     - **网络设备**：物理网络接口卡（NIC）、网线、Wi-Fi适配器、路由器、交换机等。
   - **连接方式**：
     - **有线**：以太网（RJ-45连接）。
     - **无线**：Wi-Fi（802.11标准）。
2. **数据链路层（Data Link Layer）**
   - **网络接口卡（NIC）驱动程序**：负责与物理层设备的通信。
   - **协议**：MAC地址、以太网协议、ARP（地址解析协议）。
3. **网络层（Network Layer）**
   - **协议**：IPv4、IPv6、ICMP（Internet控制消息协议）。
   - **组件**：
     - **Windows防火墙**：用于过滤传入和传出的数据包。
     - **路由表**：管理数据包的路由路径。
4. **传输层（Transport Layer）**
   - **协议**：TCP（传输控制协议）、UDP（用户数据报协议）。
   - **组件**：
     - **Windows TCP/IP协议栈**：处理传输层的数据流。
     - **端口管理器**：管理应用程序的端口使用情况。
5. **会话层（Session Layer）**
   - **协议**：NetBIOS、RPC（远程过程调用）。
   - **组件**：
     - **会话管理**：管理不同应用之间的会话。
     - **Windows会话服务**：管理用户登录会话。
6. **表示层（Presentation Layer）**
   - **数据格式**：SSL/TLS加密、数据压缩、格式转换。
   - **组件**：
     - **加密服务**：提供数据加密和解密功能。
     - **证书管理**：管理数字证书和加密密钥。

7. **应用层（Application Layer）**
    - **应用软件**：
        - **操作系统应用**：Windows自身的应用（如资源管理器、任务管理器）。
        - **第三方应用**：SQL Server、Microsoft Office、浏览器（Edge、Chrome等）、邮件客户端（Outlook）。
    - **协议**：HTTP/HTTPS、FTP、SMTP、POP3、IMAP、SQL。

TCP/IP四层模型分解

1. **网络接口层（Network Interface Layer）**
    - **硬件**：物理网络接口卡（NIC）、网线。
    - **驱动程序**：NIC驱动程序、网络适配器配置。
    - **协议**：以太网、Wi-Fi（802.11）。
2. **互联网层（Internet Layer）**
    - **协议**：IP（IPv4/IPv6）、ICMP、ARP。
    - **组件**：IP地址配置、子网掩码、默认网关设置、路由表。
3. **传输层（Transport Layer）**
    - **协议**：TCP、UDP。
    - **组件**：端口管理、连接建立与终止、数据传输控制。
4. **应用层（Application Layer）**
    - **应用软件**：
        - **操作系统应用**：Windows应用（如文件资源管理器、Windows Update）。
        - **第三方应用**：SQL Server、Microsoft Office、Web服务、邮件客户端。
    - **协议**：HTTP/HTTPS、SMTP、DNS、DHCP、SQL。

SEC2: 实现CIA的安全策略和安全机制

保密性（Confidentiality）

- **加密**：
    - **文件系统加密**：BitLocker加密整个硬盘，确保存储数据的安全。
    - **网络通信加密**：TLS/SSL用于加密HTTP、FTP等协议，确保数据在传输过程中不被窃取。
    - **实现**：BitLocker加密硬盘数据，TLS/SSL加密网络通信数据，保护数据在传输过程中的安全。
- **访问控制**：
    - **文件和目录权限**：通过NTFS文件系统设置不同用户和组的访问权限。
    - **用户账户控制（UAC）**：限制应用程序在未经授权的情况下提升权限。
    - **实现**：NTFS文件系统权限设置，用户账户控制机制防止未经授权的访问。

完整性（Integrity）

- **校验和与哈希**：
    - **数据传输校验**：TCP协议中的校验和确保传输数据的完整性。
    - **文件完整性检查**：使用MD5、SHA-256等哈希算法校验文件完整性。
    - **实现**：使用哈希算法检查文件和数据包的完整性，防止数据被篡改。
- **数字签名**：
    - **代码签名**：确保下载和执行的软件未经篡改。
    - **文档签名**：Office文档和其他重要文件的数字签名。
    - **实现**：使用数字签名技术确保软件和文件的来源可信，防止篡改。

可用性（Availability）

- **备份与恢复**：
  - **系统备份**：使用Windows Backup工具定期备份系统。
  - **SQL数据库备份**：定期备份SQL Server数据库，防止数据丢失。
  - **云备份**：使用OneDrive等云存储进行数据备份。
  - **实现**：定期备份系统和重要数据，确保在硬件故障或数据丢失时可以快速恢复。
- **冗余与容错**：
  - **RAID磁盘阵列**：使用RAID技术提高数据存储的可靠性和性能。
  - **冗余网络连接**：配置多条网络连接，保证网络的高可用性。
  - **实现**：通过RAID技术实现磁盘冗余，使用冗余网络连接确保网络的高可用性。
- **安全更新和补丁管理**：
  - **Windows Update**：定期更新操作系统，修复漏洞和提升安全性。
  - **Office和SQL Server更新**：确保应用程序的最新版本和补丁。
  - **实现**：通过定期安装操作系统和应用软件的安全补丁，防止已知漏洞被利用。

具体组件对应安全策略和机制

- **Windows防火墙**：
  - **实现**：保护网络层和传输层，防止未经授权的网络访问。
  - **对应**：可用性（Availability）、保密性（Confidentiality）。
- **BitLocker**：
  - **实现**：保护物理层和数据链路层的数据安全。
  - **对应**：保密性（Confidentiality）。
- **用户账户控制（UAC）**：
  - **实现**：防止未经授权的应用程序获取管理员权限。
  - **对应**：保密性（Confidentiality）、完整性（Integrity）。
- **数字签名和加密**：
  - **实现**：保护应用层的数据完整性和机密性。
  - **对应**：保密性（Confidentiality）、完整性（Integrity）。

通过这些详细的安全策略和机制，Windows 10-x86主机能够在操作系统、软件和硬件层面实现CIA（保密性、完整性和可用性）的安全目标。