# 三级系统建议上线安全产品及依据

## （1）边界防火墙和区域防火墙

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- |
| 网络安全 | 访问控制 | a)应在网络边界部署访问控制设备，启用访问控制功能； | 非常重要 |  |
| b)应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级； | 非常重要 |  |
| 结构安全 | f)应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段； | 非常重要 |  |
| g)应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。 | 非常重要 |  |

## （2）IDS和IPS

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- |
| 网络安全 | 入侵防范 | a)应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等； | 非常重要 |  |
| b)当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。 | 非常重要 |  |
| 访问控制 | c)应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制； | 非常重要 |  |

## （3）防病毒网关

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **备注** |
| --- | --- | --- | --- |
| 网络安全 | 恶意代码防护 | a)应在网络边界处对恶意代码进行检测和清除； |  |
| b)应维护恶意代码库的升级和检测系统的更新。 |  |
| 主机安全 | 恶意代码防范 | a)应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库； |  |
| b)主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库； |  |
| c)应支持防恶意代码的统一管理。 |  |
| 系统云纹管理 | 恶意代码防范管理 | b)应指定专人对网络和主机进行恶意代码检测并保存检测记录； |  |
| c)应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定； |  |
| d)应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。 |  |

## WEB应用防火墙（防篡改）

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- |
| 数据安全及备份恢复 | 数据完整性 | a)应能够检测到系统管理数据、鉴别信息和用户数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施； | 非常重要 | 协议校验、防篡改功能 |
| 应用安全 | 软件容错 | a)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求； | 非常重要 | 部分老旧应用无相关校验功能，可有WEB防火墙对应用请求进行合法过滤 |

## 上网行为管理系统

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **备注** |
| --- | --- | --- | --- |
| 网络安全 | 边界完整性检测 | b)应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。 |  |
| 系统运维管理 | 网络安全管理 | h)应定期检查违反规定拨号上网或其他违反网络安全策略的行为。 |  |

## （6）企业版杀毒软件

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- |
| 主机安全 | 恶意代码防范 | a)应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库； | 重要 |  |
| b)主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库； | 重要 |  |
| c)应支持防恶意代码的统一管理。 | 重要 |  |

## （7）日志审计系统

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **备注** |
| --- | --- | --- | --- |
| 网络安全 | 安全审计 | a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； |  |
| b)审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； |  |
| c)应能够根据记录数据进行分析，并生成审计报表； |  |
| d)应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 | 保持日志记录6个月 |
| 主机安全 | 安全审计 | d)应能够根据记录数据进行分析，并生成审计报表； |  |
| 应用安全 | 安全审计 | b)应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录； |  |
| d)应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。 |  |
| 系统运维管理 | 系统安全管理 | g)应定期对运行日志和审计数据进行分析，以便及时发现异常行为。 |  |

## 数据库审计

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- |
| 主机安全 | 安全审计 | a)审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户； | 重要 |  |

## 运维审计系统（堡垒机）

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- |
| 网络安全 | 网络设备防护 | d)主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别； | 非常重要 | 部分网络和安全设备不支持双因子认证、口令复杂度策略与更换策略，需要第三方运维管理工具实现 |
| e)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 非常重要 |
| 主机安全 | 访问控制 | b)应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限； | 非常重要 |  |

## 异地备份方案

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- |
| 数据安全及备份恢复 | 备份和恢复 | a)应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放； | 重要 | 这个具体怎么实现的？？ |
| b)应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地； | 重要 |

## 网络管理系统

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- |
| 主机安全 | 资源控制 | c)应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况； | 重要 | 这个就是SOC？？ |
| e)应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。 | 重要 |

## （12）网络准入系统

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- |
| 网络安全 | 边界完整性检查 | a)应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断； | 重要 | 这个是具体怎么实现的？？ |

# **二、二级系统上线安全产品及依据**

## （1）边界防火墙

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- |
| 网络安全 | 访问控制 | a)应在网络边界部署访问控制设备，启用访问控制功能； | 非常重要 |  |
| b)应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级； | 非常重要 |  |

## （2）IDS

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- |
| 网络安全 | 入侵防范 | a)应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等； | 非常重要 |  |

## （3）WEB应用防火墙（模块）

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **备注** |
| --- | --- | --- | --- |
| 数据安全及备份恢复 | 数据完整性 | a)应能够检测到系统管理数据、鉴别信息和用户数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施； | 协议校验、防篡改功能 |
| 应用安全 | 软件容错 | a)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求； |  |
| 网络安全 | 访问控制 | c)应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制； |  |

## 日志审计系统

### 主要依据

| **安全层面** | **安全控制点** | **测评指标** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- |
| 网络安全 | 安全审计 | a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； | 非常重要 |  |
| b)审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 非常重要 |  |
| 主机安全 | 安全审计 | d)应保护审计记录，避免受到未预期的删除、修改或覆盖等。 | 非常重要 | Window主机具备审计进程自我保护，linux主机？ |

## （5）运维审计系统（堡垒机）

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- |
| 网络安全 | 网络设备防护 | d)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 一般 | 部分网络和安全设备不支持双因子认证、口令复杂度策略与更换策略，需要第三方运维管理工具实现 |

## （6）数据库审计系统

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- |
| 主机安全 | 安全审计 | a)审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户； | 重要 |  |

## （7）上网行为管理系统

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- |
| 网络安全 | 边界完整性检测 | a)应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。 | 非常重要 |  |

## 企业版杀毒软件

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **备注** |
| --- | --- | --- | --- |
| 网络安全 | 恶意代码防护 | a)应在网络边界处对恶意代码进行检测和清除； |  |
| b)应维护恶意代码库的升级和检测系统的更新。 |  |
| 主机安全 | 恶意代码防范 | a)应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库； |  |
| b)主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库； |  |
| c)应支持防恶意代码的统一管理。 |  |
| 系统云纹管理 | 恶意代码防范管理 | b)应指定专人对网络和主机进行恶意代码检测并保存检测记录； |  |
| c)应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定； |  |
| d)应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。 |  |

## 本地备份方案

### 1、主要依据

| **安全层面** | **安全控制点** | **测评指标** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- |
| 数据安全及备份恢复 | 备份和恢复 | a)应能够对重要信息进行备份和恢复； | 重要 |  |

## （10）漏洞扫描

| **安全层面** | **安全控制点** | **测评指标** | **备注** |
| --- | --- | --- | --- |
| 系统运维管理 | 网络安全管理 | d)应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补； |  |
| 系统安全管理 | b)应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补； |  |