moumou系统安全管理规范

一. 目标

主机系统作为信息存储、传输、应用处理的基础设施，其自身安全性可能影响整个业务平台的安全。作为业务平台系统中重要的组成部分，各种业务系统主机数量众多，资产价值高，面临的安全风险极大。

本规范制定的目标是统一业务平台的主机系统安全技术规范，指导业务平台主机的安全配置和维护，提高业务平台各系统总体安全水平。保障公司经营活动能够持续、稳定和安全地进行，减少由信息安全风险产生的经济或名誉损失，满足国家法律和法规对公司信息安全保障能力的要求。

二. 定义和术语

身份鉴别：指在计算机及计算机网络系统中确认操作者身份的过程，从而确定该用户是否具有对某种资源的访问和使用权限，防止攻击者假冒合法用户获得资源的访问权限，保证系统和数据的安全，以及授权访问者的合法权益。

入侵防护：入侵防护是一种可识别潜在威胁并迅速地作出应对的网络安全防范办法。 恶意代码防范：恶意代码又称恶意软件。是指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装运行，侵犯用户合法权益的软件。恶意代码也指故意编制或设置的、对网络或系统会产生威胁或潜在威胁的计算机代码。

主机安全管理：系统需按安全基线配置进行安全加固，定期对系统进行扫描，并对发现的漏洞进行修复，及时对操作系统进行补丁安装。

安全审计： 信息安全审计是指对系统中与安全有关的活动的相关信息进行识别、记录、存储和分析。

三. 适用范围

3.1 人员范围

集团研发人员、集团运维部门、集团安全部门。

3.2 系统范围

集团所有的主机，包括生产环境、测试环境和开发环境等部署的操作系统及应用系统。

1. 规范详情和职责分工

4.1 主机安全管理

4.1.1 系统初始化

系统初始化时由运维部门根据集团主机安全配置指南进行主机加固设置， 保证运行环境

的基础安全。 初始化默认配置要求：

l 采用最小权限原则， 安装软件最小化、目录文件权限最小化、用户权限最小化、程

序权限运行最小化；

l 不使用的软件默认不安装；

l 危险工具默认不安装， 详情参考危险工具列表；

l 主机命名规范：主机位置+机房名称+业务线+服务；

l 禁用匿名账号；

l 禁止对外开放敏感服务，详情参考附件中敏感服务列表；

l 按照《基线配置文档》优化系统参数。

4.1.2 系统统一管理

集团所有的云主机、 IDC 主机， 包括生产环境、测试环境和开发环境等必须通过堡垒机

进行登录，由运维部门进行统一规范管理，操作系统管理员由运维部领导指定专人担任。

4.1.3 堡垒机

集团所有的云主机、 IDC 主机， 包括生产环境、测试环境和开发环境等不允许直接登录 （ssh 或 rdp） ，必须通过堡垒机进行跳转登录。关于堡垒机的使用运维部门须遵循以下安

全规范：

l 访问堡垒机需要拨集团 VPN；

l 登录堡垒机， 采用双因素认证；

l 堡垒机需满足对人员操作行为的控制和审计。

4.1.4 系统服务

操作系统中默认开启很多不必要的服务， 考虑到系统的安全性， 运维部门须遵循以下安

全规范：

l 遵循最小安装的原则，仅安装需要的组件和应用程序；

l 关闭不需要的系统服务、 默认共享，减小系统负荷，降低风险；

l 禁止开放共享目录或共享文件等共享服务；

l 禁止对外开放 MySQL、SSH、FTP 等高危服务， 详情参考附件中敏感服务端口列表；

l 危险的 Linux 工具， 根据最佳的安全实践和对攻击载荷的分析，命令列表如下：

|  |  |  |
| --- | --- | --- |
| 工具或操作 | 危害举例 | 管理方式 |
| Nc | 反弹 shell，创建隧道 | 默认禁用 |
| Netcat | 反弹 shell，创建隧道 | 默认禁用 |
| Socat | 反弹 shell，创建隧道 | 默认禁用 |
| history -c | 清除命令历史记录 | 默认禁用 |
| Lcx | 隧道转发 | 默认禁用 |
| Ircdproxy | 隧道转发 | 默认禁用 |
| Ssserver | 端口代理 | 默认禁用 |
| shadowsocks | 端口代理 | 默认禁用 |
| Scp | 远程传输 | 建议禁用 |
| Shadow | 超敏感文件 | 特权用户访问 |
| Passwd | 超敏感文件 | 特权用户访问 |
| Ettercap | 网络嗅探 | 建议禁用 |
| Arpsniffer | arpsniffer 进行 arp 欺骗 | 默认禁用 |
| Hydra | 内网横向扫描 | 默认禁用 |

4.1.5 安全基线

安全基线是一个信息系统的最小安全保证，即该信息系统最基本需要满足的安全要求。 系统上线前， 运维部门应参照《安全配置指南》 对主机系统、应用、数据库等进行安全

加固。 操作系统管理员每半年应根据 《安全配置指南》 对系统基线设置进行复核。

4.1.6 系统补丁

对于操作系统， 安全漏洞的存在是不可避免的， 因此需要针对系统的缺陷进行漏洞的修 补，但考虑到补丁与现有业务系统的兼容性不能盲目地进行漏洞修补， 漏洞的修复工作需要

慎重操作，主机系统的漏洞补丁升级需要满足以下技术要求：

l 须安装漏洞扫描工具， 实现定期漏洞扫描 （每月至少一次） ，识别 Linux 软件漏 洞、 Windows 系统漏洞、 第三方软件漏洞； 由安全部门评估主机的漏洞级别（高 危、中危、低危） ，运维部门协助研发部门根据扫描结果对漏洞进行修复，漏洞

修复要求如下：

n 低危漏洞-V1 级：需要在 7 天内修复漏洞并反馈。

n 中危漏洞-V2 级：需要在 3 天内修复漏洞并反馈。

n 高危漏洞-V3 级：需要在 1 天内修复漏洞并反馈。

l 对于集团安全部门发布的安全预警信息，由运维部门协助研发部门对漏洞进行修 复；

l 更新补丁前，应对补丁与现有业务系统的兼容性进行测试，记录测试过程及结 果，并通过直属领导审批后，从测试环境开始修补，确认补丁可靠后分批次对其 他环境进行修复；

l 安装补丁软件包以必要为原则，非必要的包不安装。

4.2 鉴别与控制

4.2.1 访问控制

远程访问用于服务器的远程控制， 用户从任何一点就可以远程控制主机系统， 方便用户

的操作， 但很容易受到恶意攻击或利用。

考虑到远程访问控制的高风险， 需要设置安全的访问控制， 运维部门负责访问控制管理

工作，应满足以下需求：

l 禁止匿名用户登录；

l 禁止用户通过 ssh、rdp 等方式直接登录服务器，必须通过堡垒机进行访问，并且 登录堡垒机时需要拨集团 VPN；

l 对用户进行严格的访问控制， 根据用户角色 （特权用户、运维用户、 普通用户） 授 权相应权限， 实现管理用户的职责分离；

l 具有登录失败处理功能， 如一分钟 3 次登录失败则锁定 30 分钟； 还应配置并启用 结束会话、登录连接超时自动退出等相关措施， 时间设置参数应为 10 分钟以内；

l 支持设置某一用户可以进行的最大连接数， 建议个人用户 （例如： 张三） 连接数不 超过 3，公共用户 （例如： dev） 连接数不超过 6；

l 进行远程管理时， 应采取必要措施， 防止鉴别信息在网络传输过程中被窃听。例如：

进行远程管理时，需要使用 VPN，禁止使用ssh 进行直接认证操作。

4.2.2 身份鉴别

由于主机系统承载着应用系统重要的业务和数据信息， 对于业务平台系统资产重要性和

保护力度来说是重中之重， 因此应采用严格身份鉴别技术用于主机系统用户的身份鉴别。运

维部门负责身份鉴别管理工作，应满足以下需求：

l 对登录操作系统和数据库系统的用户进行身份鉴别；

l 根据用户的角色分配不同权限， 实现用户职责分离。设定角色权限：

n 管理员：具备所有权限；

n 运维用户：具备相关服务控制管理权限以及部分系统权限；

n 普通用户： 用于登录服务器查看业务日志、配置以及运行一些简单脚本，

有权读取、无权操纵管理线上业务服务及系统配置。

4.2.3 账号与口令

系统安全的一个重要方面是对有管理权限访问计算机资源， 或者服务的用户和组进行管

理，从操作系统账号角度出发，运维部门、集团研发部门负责满足账号管理要求如下：

l 修改默认账号的默认口令；

l 定期删除或停用多余的、过期的账号，避免共享账号的存在；

l 新增账户需要相关领导审核确认后赋予相关角色权限；

l 采用合适的安全措施， 严格进行主机系统口令文件的保存， 如本地保存需对文本进 行加密处理、 禁止把密码放在第三方开放平台 （如 github，未知笔记等）；

l 口令应遵循《moumou信息安全规定》 要求，满足 8 位及以上长度，含大小写

字母、数字和特殊字符，每 90 天更新一次。

4.3 入侵检测与防范

针对业务平台中 Windows、Linux 主机系统需要采用适当的主机入侵检测系统进行入侵 行为的检测与防护。主机入侵检测系统的选型有安全部门负责，部署实施由运维部门负 责，研发部门需要在一周内发起部署申请否则有安全部门强制要求部署。

主机入侵检测系统的功能应满足如下要求：

l 及时发现主机可能存在的安全风险 （如暴力破解、异常登录、反弹shell、后门 检测、配置不当、弱口令等） ，并及时告警； 安全部门评估后漏洞级别（高危、 中危、低危） ，运维部门和研发部门根据漏洞报告对漏洞进行修复，漏洞修复要 求如下：

n 低危漏洞-V1 级：需要在 7 天内修复漏洞并反馈。

n 中危漏洞-V2 级：需要在 3 天内修复漏洞并反馈。

n 高危漏洞-V3 级：需要在 1 天内修复漏洞并反馈。

l 对已经发生的入侵行为进行检测和实时告警，记录时间、攻击目的、攻击来源 IP、

攻击类型、攻击手段等， 及时对入侵事件进行通知和处理， 具体请参考《moumou信息安全规定》 中安全事件的管理办法。

4.4 恶意代码防护

4.4.1 恶意代码防范

业务平台中 Windows、Linux 主机系统必须具备防范病毒、木马等恶意代码的能力。恶 意代码防护系统的选型由安全部门负责，部署实施由运维部门负责，集团研发需要在主机

上线一周内安排部署，逾期将强制要求部署。

恶意代码防护系统应满足如下要求：

l 具备实时监测和查杀恶意代码的能力，能够发现恶意事件（挖矿、木马、 webshell等） ，定期对系统中的程序或数据文件进行病毒检查；针对安全事件的

处理， 参考《moumou信息安全规定》 中安全事件管理；

l 恶意代码防护系统应由安全部门设置统一的防护策略，自动保持防恶意代码规则 库的更新

l 系统管理员通过人工或者系统自动化方式定期完成软件补丁和病毒库的更新。

4.5 安全审计

针对业务平台中 Windows、Linux 主机系统需要安装安全审计软件，对系统和数据库进 行操作审计。 审计软件选型和日志审计由安全部门负责，部署实施由运维部门负责。

审计软件系统应满足如下要求：

l 审计内容至少包括事件日期， 时间，类型，用户行为，重要系统命令的使用等事 件；

l 安全部门对日志进行审计分析和告警；

l 审计日志需远程备份。

moumou 2020 年 11 月