附件

网络和数据安全风险隐患排查表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 类别 | 检查点 | 自查情况 | 备注（检查范围和检查方式） |
| 1 | 安全  防护 | 是否安装防恶意代码或防病毒产品，是否对恶意代码进行检测和清除，并及时进行病毒库的升级和更新 |  | 检查范围：业务系统、办公终端  检查方式：配置核验 |
| 2 | 是否使用多层防护措施来确保网络安全，并进行合理化配置，如入侵检测系统、安全审计措施等 |  | 检查范围：云平台  检查方式：人员访谈、配置核验 |
| 3 | 是否使用相关安全防护措施，如防火墙、入侵检测等，并进行合理化配置 |  | 检查范围：业务系统  检查方式：人员访谈、配置核验 |
| 4 | 是否监控系统的网络流量，检查是否存在可疑网络连接和网络行为，并及时进行事件闭环处置 |  | 检查范围：云平台/业务系统、办公终端  检查方式：人员访谈、工具检查 |
| 5 | 是否对登录的用户分配账户和权限，是否授予管理用户所需的最小权限，实现管理用户的权限分离 |  | 检查范围：云平台、业务系统  检查方式：配置核验、文档查看 |
| 6 | 运维  管理 | 第三方运维人员在运维操作前是否进行授权审批确认，是否有远程运维，是否采用安全的措施开展远程运维 |  | 检查范围：业务系统  检查方式：人员访谈、文档查看  、配置核验 |
| 7 | 是否及时对操作系统补丁进行升级 |  | 检查范围：业务系统  检查方式：配置核验 |
| 8 | 是否配置和使用安全的密码规则 |  | 检查范围：业务系统  检查方式：配置核验 |
| 9 | 是否针对密码策略时长进行有效期限制，并禁止弱口令和共享密码 |  | 检查范围：业务系统  检查方式：配置核验 |
| 10 | 运维  管理 | 是否存在弱口令、默认口令、空口令 |  | 检查范围：业务系统  检查方式：配置核验 |
| 11 | 是否能发现可能存在的安全漏洞，并在经过充分测试评估后及时修补安全漏洞 |  | 检查范围：业务系统  检查方式：人员访谈、工具检查 |
| 12 | 是否针对自身网络资产进行资产台账梳理识别，明确资产内容，如资产编号、终端、服务器/虚拟机等、IP、操作系统及版本、所属部门、责任人等 |  | 检查范围：业务系统  检查方式：人员访谈、文档查看 |
| 13 | 是否建立巡检机制，定期检查CPU、内存使用率过高的情况，是否存在可疑启动项、服务启动、计划任务 |  | 检查范围：业务系统  检查方式：人员访谈、配置核验 |
| 14 | 策略  配置 | 是否通过防火墙等技术手段封禁非必要端口，如22、139、445、1433、3306、3389、6379等 |  | 检查范围：云平台/业务系统  检查方式：配置核验 |
| 15 | 互联网区与政务外网区是否采取网闸等措施进行有效物理隔离，业务系统内部是否按照建设要求对不同的网络区域进行有效逻辑隔离 |  | 检查范围：云平台、业务系统  检查方式：人员访谈、配置核验  、文档查看 |
| 16 | 安全设备是否更新为最新版本，避免发生安全设备漏洞利用 |  | 检查范围：云平台、业务系统  检查方式：配置核验 |
| 17 | 是否存在不合理的远程桌面服务 |  | 检查范围：业务系统  检查方式：配置核验 |
| 18 | 数据  安全 | 是否提供重要数据的本地数据备份与恢复功能，是否开展数据恢复有效性验证 |  | 检查范围：业务系统  检查方式：人员访谈、配置核验 |
| 19 | 是否开启记录并审计系统事件日志 |  | 检查范围：业务系统（数据库）  检查方式：人员访谈、配置核验 |
| 20 | 审计日志、数据库日志等日志留存是否不少于六个月 |  | 检查范围：业务系统（数据库）  检查方式：人员访谈、配置核验 |
| 21 | 是否限制数据库远程连接方式或IP地址 |  | 检查范围：业务系统（数据库）  检查方式：人员访谈、配置核验 |
| 22 | 数据  安全 | 数据库账户是否存在过期账户、无关账户 |  | 检查范围：业务系统（数据库）  检查方式：人员访谈、配置核验 |
| 23 | 是否采用密码技术，保证重要数据在传输、存储过程中的保密性、完整性 |  | 检查范围：业务系统  检查方式：人员访谈、配置核验 |