###### Windows操作系统基线配置脆弱性整改建议

|  |  |  |  |
| --- | --- | --- | --- |
| **项目**  **编号** | **安全基线检查项目** | **安全基线检查说明** | **安全基线检查符合性判定依据** |
| W-JX-01 | 缺省帐号 | 对于管理员帐号，要求更改缺省帐号名称；  禁用guest（来宾）帐号； | 1. 更改缺省账户Administrator 名称； 2. 禁用guest（来宾）账号 |
| **（IP2）安全基线检查结果及配置现状截图：** | | | |
| **（IP2）整改说明并附截图：** | | | |
| W-JX-02 | 无用帐号 | 删除或锁定与设备运行、维护等与工作无关的帐号； | 结合要求和实际业务情况判断符合要求，删除或锁定与设备运行、维护等与工作无关的帐号； |
| **（IP2）安全基线检查结果及配置现状截图：** | | | |
| **（IP2）整改说明并附截图：** | | | |
| W-JX-03 | 用户权限分离 | 按照用户分配帐号。根据系统的要求，设定不同的账户和账户组，管理员用户，操作员用户operator，审计用户auditor 等； | 结合要求和实际业务情况判断符合要求，根据系统的要求，设定不同的账户和账户组，管理员用户，操作员用户，审计用户；  **管理员账号：**分配和管理数据库其他账号密码权限；  **审计账号：**只授予访问数据库日志的权限，无法对日志进行操作；  **操作员：**安全管理员，配置数据库策略，或者拥有账号管理权限；  **业务账号：**普通账号，用来创建应用或者数据库； |
| **（IP2）安全基线检查结果及配置现状截图：** | | | |
| **（IP2）整改说明并附截图：** | | | |
| W-JX-04 | 密码复杂度 | 最短密码长度12 个字符，启用本机组策略中密码必须符合复杂性要求的策略。即密码需要包含以下四种类别的字符：  英语大写字母:A,B,…Z  英语小写字母a,b,…z  西方阿拉伯数字0,1,…9  非字母数字字符，如标点符号，@, #, $, %, &, \* 等 | 本地安全策略-账户策略-密码策略：  1、“密码必须符合复杂性要求”选择“已启动”；  2、密码长度最小值：12个字符 |
| **（IP2）安全基线检查结果及配置现状截图：** | | | |
| **（IP2）整改说明并附截图：** | | | |
| W-JX-05 | 密码最长生存期 | 对于采用静态口令认证技术的系统，账户口令的生存期不长于90 天。 | 本地安全策略-本地策略-安全选项：  进入“控制面板->管理工具-> 本地安全策略”，在“帐户策略->密码策略”：“密码最长使用期限”设置不大于“90天” |
| **（IP2）安全基线检查结果及配置现状截图：** | | | |
| **（IP2）整改说明并附截图：** | | | |
| W-JX-06 | 密码历史记录 | 对于采用静态口令认证技术的设备，应配置设备，使用户不能重复使用最近5次（含5次）内已使用的口令。 | 本地安全策略-本地策略-安全选项：  进入“控制面板->管理工具-> 本地安全策略”，在“帐户策略->密码策略”：查看是否“强制密码历史”设置为“记住5个密码” |
| **（IP2）安全基线检查结果及配置现状截图：** | | | |
| **（IP2）整改说明并附截图：** | | | |
| W-JX-07 | 帐号锁定策略 | 对于采用静态口令认证技术的设备，应配置当用户连续认证失败次数超过3次，锁定该用户使用的帐号。 | 本地安全策略-本地策略-账户锁定策略：  “账户锁定阀值”设置为小于或等于3次，锁定时间5分钟。 |
| **（IP2）安全基线检查结果及配置现状截图：** | | | |
| **（IP2）整改说明并附截图：** | | | |
| W-JX-08 | 远程关机权限 | 在本地安全设置中从远端系统强制关机只指派给Administrators 组 。 | 本地安全策略-本地策略-用户权限分配：“从远端系统强制关机”设置为“只指派给Administrtors组” |
| **（IP2）安全基线检查结果及配置现状截图：** | | | |
| **（IP2）整改说明并附截图：** | | | |
| W-JX-09 | 本地关机权限 | 在本地安全设置中关闭系统仅指派给Administrators组。 | 本地安全策略-本地策略-用户权限分配：“关闭系统”设置为“只指派给Administrators 组 ” |
| **（IP2）安全基线检查结果及配置现状截图：** | | | |
| **（IP2）整改说明并附截图：** | | | |
| W-JX-10 | 隐藏上次登录名 | 交互式登录，不显示上次登录的用户名 | 本地安全策略-本地策略-安全选项：“交互式登录:不显示最后的用户名”设置为“已启用” |
| **（IP2）安全基线检查结果及配置现状截图：** | | | |
| **（IP2）整改说明并附截图：** | | | |
| W-JX-11 | 关机清理内存页面 | 关机时清理虚拟内存页面文件 | 本地安全策略-本地策略-安全选项：“关机 ：清理虚拟内存页面文件”设置为“已启用” |
| **（IP2）安全基线检查结果及配置现状截图：** | | | |
| **（IP2）整改说明并附截图：** | | | |
| W-JX-12 | 用户权利指派 | 在本地安全设置中取得文件或其它对象的所有权仅指派给Administrators 。 | 本地安全策略-本地策略-用户权限分配：“取得文件或其它对象的所有权”设置为“只指派给Administrators组” |
| **（IP2）安全基线检查结果及配置现状截图：** | | | |
| **（IP2）整改说明并附截图：** | | | |
| W-JX-13 | 本地审核策略 | 设备应配置日志功能，对策略更改、登录事件、对象访问、进程跟踪、目录服务访问、特权使用、系统事件、帐号登录事件、帐号管理事件进行审核记录。 | 本地安全策略-本地策略-审核策略：  审核策略更改：成功，失败  审核登录事件：成功，失败  审核对象访问：无审核  审核进程跟踪：无审核 审核目录服务访问：失败  审核特权使用：失败  审核系统事件：成功，失败  审核帐号登录事件：成功，失败  审核帐号管理：成功，失败 |
| **（IP2）安全基线检查结果及配置现状截图：** | | | |
|  | | | |
| W-JX-14 | 日志文件大小 | 设置应用日志文件大小至少为200M，设置当达到最大的日志尺寸时，按需要改写事件。 | 管理工具-事件查看器：“应用日志”“系统日志”“安全日志”属性中的日志大小设置不小于“200M”,设置当达到最大的日志尺寸时，“按需要改写事件”。 |
| **（IP2）安全基线检查结果及配置现状截图：** | | | |
| **（IP2）整改说明并附截图：** | | | |
| W-JX-15 | 防病毒管理 | 对服务器主机应当安装部署服务器专版杀毒软件，并打开自动升级病毒库选项。 | 点击进入杀毒软件的操作界面，检查是否开启自动更新。如不存在杀毒软件或者没打开自动更新即为不合规。 |
| **（IP2）安全基线检查结果及配置现状截图：** | | | |
| **（IP2）整改说明并附截图：** | | | |
| W-JX-16 | 补丁更新 | 安装最新的Windows操作补丁补丁集 | 应设置升级服务器等方式保持系统补丁及时得到更新  注意：安装补丁存在一定的风险，打上补丁后重启系统前，应该备份系统上的重要数据及程序，不把备份的数据放在本服务器 |
| **（IP2）安全基线检查结果及配置现状截图：** | | | |
| **（IP2）整改说明并附截图：** | | | |
| W-JX-17 | 系统防火墙 | 应开启系统防火墙功能 | 启用工作网络位置防火墙设置，启用公用网络位置防火墙设置。 |
| **（IP2）安全基线检查结果及配置现状截图：** | | | |
| **（IP2）整改说明并附截图：** | | | |
| **配置影响地址** | | | |
|  | | | |