|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **版本** | **更改日期** | **要点说明** | **编制** | **审核** | **批准** |
| V1.0 | 2018-4-23 | 拟定数广侧windowsOS加固配置规范 | Cheungwu |  |  |
| 文档保密等级： | | □机密 ■内部 □公开 | | | |

注：请在所属的选项□上，用黑色突出标识。示例：■内部

# 操作系统安全配置

* 1. 服务器版本必须是window 2008R2及以上版本；
  2. 服务器须安装杀毒软件，并确保杀毒软件正常运行；
  3. 服务器须及时安装安全补丁，修复高危漏洞；

1.3.1高危漏洞，可造成远程代码任意执行的，须每月微软补丁日一周内完成安全补丁安装；

1.3.2其它漏洞，须按照部门统一要求，定期在变更窗口内进行安全补丁安装。

# 服务器帐号要求

1. 1 应用程序使用的系统帐号不能有登陆操作系统的权限；

安全策略设置权限分配

gpedit.msc->computer configuration->windows settings->local policy中allow log on locally、allow log on through remote desktop service中配置

1. 2 服务器须创建实名制系统帐号，并通过实名制帐号来登陆维护。默认禁止非实名制帐号登陆。

安全策略设置权限分配

gpedit.msc->computer configuration->windows settings->local policy中allow log on locally、allow log on through remote desktop service中配置

2.3 服务器本地管理员密码策略需符合以下要求：

1)不能包含用户的帐户名，不能包含用户姓名中超过两个连续字符的部分

2)至少有八个字符长

3)包含以下四类字符中的三类字符:

英文大写字母(A 到 Z)

英文小写字母(a 到 z)

10 个基本数字(0 到 9)

非字母字符(例如 !、$、#、%)

4)密码长度最小值：8个字符

5)密码最长使用期限：90天

6)强制密码历史：记住5个历史密码

7)帐户锁定阀值：30次无效登陆

8)帐户锁定时间：30分钟

9)重置帐户锁定计数器：30分钟

安全策略设置

gpedit.msc->computer configuration->windows settings->account policy->password policy中设置

2.4.WINDOWS服务器本地用户须禁用无效帐户，如Guest，并对业务设立专有维护帐号。

计算机管理中设置

2.5.根据系统的要求，设定不同的帐户和帐户组，管理员用户，数据库用户，审计用户，来宾用户等。避免帐号混淆，权限不明确，存在用户越权使用的可能。

2.6.删除或锁定与设备运行、维护等与工作无关的帐号，提高系统帐户安全。

2.7.设置本地帐号锁定策略，30次错误验证后锁定本地帐号30分钟。

安全策略设置

gpedit.msc->computer configuration->windows settings->account policy->account logout policy中设置

2.8.只允许WINDOWS服务器管理员帐户从本地或远程登陆服务器。

安全策略设置权限分配

gpedit.msc->computer configuration->windows settings->local policy中allow log on locally、allow log on through remote desktop service中配置

# 日志配置要求

3.1设置审核策略，记录系统重要的事件日志。对用户登录进行记录，记录内容包括用户登录使用的帐号，登录是否成功，登录时间，以及远程登录时，用户使用的IP地址；对进程进行记录。

安全策略设置审核

gpedit.msc->computer configuration->windows settings->local policy –>audit policy和gpedit.msc->computer configuration->windows settings->advanced audit policy configuration中配置

# 关闭高危服务

4.1.关闭服务器远程注册表、自动播放、ICS高危服务。

服务中关闭remote registry和ICS服务

gpedit.msc->computer configuration->administrative templates->windows components->autoplay policies->turn off autoplay 设置为true

4.2.与业务无关的服务须关闭，如samba服务、FTP。

检查45、21端口是否开启

# 配置主机防火墙

5.1启用主机防火墙，入站和出站均默认阻止，应用至域配置文件、专用配置文件和公用配置文件。

5.2设置入站方向策略,仅允许指定的业务端口被指定的来源IP访问。

# 简明checklist

|  |  |  |  |
| --- | --- | --- | --- |
| 分类 | 检查点 | 检查方法 | 检查结果 |
| 操作系统安全配置 | 服务器版本必须是window 2008R2及以上版本 | 检查服务器版本 |  |
| 服务器须安装杀毒软件，并确保杀毒软件正常运行 | 检查杀软运行情况 |  |
| 服务器须及时安装安全补丁，修复高危漏洞 | 检查安全补丁列表 |  |
| 服务器帐号要求 | 应用程序使用的系统帐号不能有登陆操作系统的权限 | gpedit.msc->computer configuration->windows settings->local policy中allow log on locally、allow log on through remote desktop service中配置 |  |
| 禁止非实名制帐号登陆 | gpedit.msc->computer configuration->windows settings->local policy中allow log on locally、allow log on through remote desktop service中配置 |  |
| 服务器本地管理员密码策略设置 | gpedit.msc->computer configuration->windows settings->account policy->password policy中设置 |  |
| 禁用无效帐户，如Guest | 计算机管理中设置 |  |
| 设定不同的帐户和帐户组，管理员用户，数据库用户，审计用户，来宾用户等。避免帐号混淆，权限不明确，存在用户越权使用的可能 | 系统管理员自检 |  |
| 删除或锁定与设备运行、维护等与工作无关的帐号，提高系统帐户安全 | 系统管理员自检 |  |
| 本地帐号锁定策略，30次错误验证后锁定 | gpedit.msc->computer configuration->windows settings->account policy->account logout policy中设置 |  |
| 只允许WINDOWS服务器管理员帐户从本地或远程登陆服务器 | gpedit.msc->computer configuration->windows settings->local policy中allow log on locally、allow log on through remote desktop service中配置 |  |
| 日志配置要求 | 记录系统重要的事件日志 | gpedit.msc->computer configuration->windows settings->local policy –>audit policy  和  gpedit.msc->computer configuration->windows settings->advanced audit policy configuration中配置 |  |
| 关闭高危服务 | 关闭服务器远程注册表、自动播放、ICS高危服务 | 服务中关闭remote registry和ICS服务  gpedit.msc->computer configuration->administrative templates->windows components->autoplay policies->turn off autoplay 设置为true |  |
| 关闭业务无关的服务，如samba服务、FTP | 检查445、21端口是否开启  netstat -ao |  |
| 配置主机防火墙 | 仅允许指定的业务端口被指定的来源IP访问 | 检查防火墙配置 |  |

\