**重点排污单位自动监控与基础数据库系统怀化市级平台网络安全隐患整改情况报告**

2021年10月8日

1. 概述

自2021年10月8日接到怀化市生态环境局下发的《安全计算环境层面问题和整改建议》后，我公司即刻组织人力，针对检查后发现的问题，迅速修补安全漏洞，并对所属网站服务器、应用系统和数据库进行彻底检查，进一步完善安全防范措施，提高网络安全防范意识，有效增强了重点排污单位自动监控与基础数据库系统怀化市级平台对有害信息的防范能力和防泄密水平。

1. 整改情况

2.1.1服务器和终端弱口令问题

1）问题描述

服务器、终端未满足口令复杂度校验机制，存在弱口令和相同口令，未定期更换口令。

1. 整改情况

对windows操作系统开启本地安全策略-账户策略-密码策略，启用密码复杂性要求，设置密码最小长度为8个字符；对Windows操作系统进行加固，开启本地安全策略-账户策略-密码策略：密码必须符合复杂性要求 已启用，密码长度最小值：8个字符，密码最长使用期限：90天。

2.1.2服务器登陆失败及超时问题

1. 问题描述

操作系统无登录失败处理功能，操作系统未设置超时。

1. 整改情况

开启终端Windows操作系统账户策略-账户锁定策略，账户锁定阈值为5次，账户锁定时间为30分钟；开启终端Windows操作系统屏幕保护程序，结合业务需求，设置屏保等待时间，如15分钟，并勾选“恢复时显示登录屏幕”。

2.1.3服务器未开启审计策略

1. 问题描述

服务器未开启审核策略。

1. 整改情况

开启服务器审核功能，如：控制面板-管理工具-安全策略-本地安全策略-审核策略下开启全部审核功能。

2.1.4服务器未将审计记录及日志上传至审计设备

1. 问题描述

服务器、终端、审计记录未上传至日志审计设备中进行集中保护。

1. 整改情况

建议市局提供专门设备将服务器、终端审计日志上传至日志审计设备中进行集中保护。

2.1.5服务器存在高危端口问题

1. 问题描述

服务器开启了135 、137、445等高危端口。

1. 整改情况

加强服务器的管理，禁用不需要的服务；通过注册表关闭磁盘默认共享；通过系统防火墙或IP安全策略设置策略禁用高危端口通信。

2.1.6应用系统弱口令问题

1. 问题描述

数据库、应用系统未满足口令复杂度校验机制，存在弱口令和相同口令，未定期更换口令。

1. 整改情况

开启Oracle数据库“PASSWORD\_VERIFY\_FUNCTION ”函数，设置口令强度策略，或使用第三方加固系统加固；对SQLServer数据库所在Windows服务器操作系统进行加固；在应用系统加入密码复杂度校验机制，如口令长度≥8，由大小写、数字和特殊字符其中三类组成（最低要求：长度大于6，由字母和数字组成）；每90天定期更换操作系统、数据库和应用系统管理账户的口令；开启MySQL数据库“validate password”插件，设置口令强度策略。

2.1.7应用系统登陆失败及超时问题

1. 问题描述

数据库、应用系统未开启登录失败策略，可输入多次错误口令；操作系统开启设置屏保功能，服务器操作未设置远程超时退出功能。

1. 整改情况

对部署数据库的服务器设置登录失败处理功能和空闲会话超时自动退出操作界面；对应用系统设置登录失败处理机制，如登录失败5次，锁定该账户10分钟。

2.1.8应用系统未采用加密技术

1. 问题描述

应用系统远程管理时采用http登陆管理，数据明文传输，未采用加密技术防止鉴别信息在网络传输过程中被窃听。

1. 整改情况

建议应用系统采取外部加密机制或采用https登录方式，防止鉴别信息在网络传输过程中被窃听。

2.1.9数据库未将审计记录及日志上传至审计设备

1. 问题描述

数据库审计记录未上传至日志审计设备中进行集中保护。

1. 整改情况

建议市局提供专门设备将服务器、终端审计日志上传至日志审计设备中进行集中保护。

2.1.10应用系统通信未采用加密

1. 问题描述

未采用密码技术进行通信完整性验证。

1. 整改情况

建议为业务应用系统配置SSL证书/HTTPS证书。

2.1.11个人信息问题

1. 问题描述

单位未制定公民个人信息在信息系统收集中的相关管理制度。

1. 整改情况

建议结合行业或主管部门相关法律法规制定个人信息管理流程或制度，对应用系统所需的个人信息的收集、使用、存储和授权等方面进行规范化管理。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 关联资产 | 风险值 | 问题描述 | 整改建议 | 是否解决 |
| 交换服务器、数据库服务器、应用服务器 | 高 | 服务器、终端未满足口令复杂度校验机制，存在弱口令和相同口令，未定期更换口令。 | 1、建议对windows操作系统开启本地安全策略-账户策略-密码策略，启用密码复杂性要求，设置密码最小长度为8个字符；2、建议对Windows操作系统进行加固，开启本地安全策略-账户策略-密码策略：密码必须符合复杂性要求 已启用，密码长度最小值：8个字符，密码最长使用期限：90天。 | 已解决 |
| 交换服务器、数据库服务器、应用服务器 | 高 | 操作系统无登录失败处理功能，操作系统未设置超时。 | 1.建议开启终端Windows操作系统账户策略-账户锁定策略，账户锁定阈值为5次，账户锁定时间为30分钟；2.建议开启终端Windows操作系统屏幕保护程序，结合业务需求，设置屏保等待时间，如15分钟，并勾选“恢复时显示登录屏幕”。 | 已解决 |
| 交换服务器、数据库服务器、应用服务器 | 高 | 服务器未开启审核策略。 | 建议开启服务器审核功能，如：控制面板-管理工具-安全策略-本地安全策略-审核策略下开启全部审核功能。 | 已解决 |
| 交换服务器、数据库服务器、应用服务器 | 高 | 服务器、终端、审计记录未上传至日志审计设备中进行集中保护。 | 建议市局提供专门设备将服务器、终端审计日志上传至日志审计设备中进行集中保护。 |  |
| 交换服务器、数据库服务器、应用服务器 | 高 | 服务器开启了135 、137、445等高危端口及默认共享。 | 建议加强服务器的管理，禁用不需要的服务；通过注册表关闭磁盘默认共享；通过系统防火墙或IP安全策略设置策略禁用高危端口通信。 | 已解决 |
| 重点排污单位自动监控与基础数据库系统、SQL Server数据库 | 高 | 数据库、应用系统未满足口令复杂度校验机制，存在弱口令和相同口令，未定期更换口令。 | 1、建议开启Oracle数据库“PASSWORD\_VERIFY\_FUNCTION ”函数，设置口令强度策略，或使用第三方加固系统加固；2、建议对SQLServer数据库所在Windows服务器操作系统进行加固；3、建议在应用系统加入密码复杂度校验机制，如口令长度≥8，由大小写、数字和特殊字符其中三类组成（最低要求：长度大于6，由字母和数字组成）；4、建议每90天定期更换操作系统、数据库和应用系统管理账户的口令。3、建议开启MySQL数据库“validate password”插件，设置口令强度策略。 |  |
| 重点排污单位自动监控与基础数据库系统、SQL Server数据库 | 高 | 数据库、应用系统无登录失败处理功能，操作系统未设置超时。 | 1、建议对部署数据库的服务器设置登录失败处理功能和空闲会话超时自动退出操作界面；2、建议对应用系统设置登录失败处理机制，如登录失败5次，锁定该账户10分钟。 |  |
| 重点排污单位自动监控与基础数据库系统、SQL Server数据库 | 高 | 应用系统远程管理时采用http登陆管理，数据明文传输，未采用加密技术防止鉴别信息在网络传输过程中被窃听。 | 建议应用系统采取外部加密机制或采用https登录方式，防止鉴别信息在网络传输过程中被窃听。 |  |
| SQL Server数据库 | 高 | 数据库审计记录未上传至日志审计设备中进行集中保护。 | 建议将数据库审计日志上传至日志审计设备中进行集中保护。 |  |
| 重点排污单位自动监控与基础数据库系统 | 高 | 未采用密码技术进行通信完整性验证。 | 建议为业务应用系统配置SSL证书/HTTPS证书。 |  |
| 重点排污单位自动监控与基础数据库系统、SQL Server数据库 | 高 | 单位未制定公民个人信息在信息系统收集中的相关管理制度。 | 建议结合行业或主管部门相关法律法规制定个人信息管理流程或制度，对应用系统所需的个人信息的收集、使用、存储和授权等方面进行规范化管理。 |  |
| 重点排污单位自动监控与基础数据库系统、SQL Server数据库 | 高 | 单位内部未制定对个人信息进行保护的相关管理制度。 | 建议结合行业或主管部门相关法律法规制定个人信息管理流程或制度，对应用系统所需的个人信息的收集、使用、存储和授权等方面进行规范化管理。 |  |