中共常州市委网络安全和信息化委员会办公室

关于做好网络设备安全管理的通知

市各有关单位，各辖市（区）委网信办，常州经开区党群工作部：

近日，某黑客组织在互联网上发布了一份涵盖515000多台服务器、家庭路由器和物联网智能设备的远程登录Telnet凭据列表，内容包含每台设备的IP地址以及Telnet服务的用户名和密码，这是迄今为止已知的最大Telnet密码泄漏事件。为进一步做好我市网络安全管理工作，切实提高网络安全防护水平，现将网络设备安全管理具体要求通知如下：

一、远程安全管理

禁用Telnet、HTTP服务，如需远程服务可启用SSH、HTTPS服务，远程管理(VTY)的登录源地址采取ACL进行限制或指定管理IP。

二、帐户管理

删除或锁定与设备运行、维护等工作无关的帐号，不同等级管理维护人员分配不同帐号，避免帐号混用。

三、密码管理

使用由数字+大小写字母+特殊字符8位以上的组合密码，开启密码加密服务，定期更新密码，严禁使用弱口令。

四、日志管理

在指定服务器保存设备日志，至少保存6个月。

五、服务管理

关闭FTP、TFTP、DNS等不必要的服务，禁用finger、bootp服务。

六、端口管理

关闭未使用的网络接口。

请各单位按照通知要求切实做好网络设备的安全管理工作，我办将组织技术力量持续监测暴露在互联网上的网络设备；如发现因网络设备未禁用Telnet服务而导致发生网络安全事件的单位，依据党委(党组)网络安全责任制实施细则的要求，我办将向实施问责的党委（党组）、纪委（纪检组）提出问责建议。

中共常州市委网络安全和信息化委员会办公室

2020年2月21日