关于加强勒索病毒防范工作的通知

省有关单位，各地级以上市政务服务数据管理局:

近期，我省发生多起政务信息系统感染勒索病毒安全事件，严重影响了政务服务和日常办公。我局高度重视，立即组织开展政务网络安全风险排查，并牵头编制了《勒索病毒防范指引》。请各地各部门切实履行网络安全党委（党组）工作责任制，进一步加强网络安全防护，有关要求通知如下:

一、进一步强化网络安全风险防范措施。各地各部门要树立底线思维，建立“以大概率思维应对小概率事件”风险防范化解机制，重点抓好信息安全、网络安全风险防范，加强网络安全监测预警、信息通报、应急处置和宣传教育等工作。

二、加强网络安全防护。各地各部门应建立健全网络安全管理制度和网络安全运营工作，对重要系统和数据库进行备份，及时监测修复网络安全漏洞，保障系统连续正常运行。

三、加强网络安全风险排查。经初步判断，本次攻击传播路径是利用 windows 远程桌面服务弱口令以及“永恒之蓝”(MS17-010)漏洞，通过系统账号密码暴力破解和漏洞利用两种途径拿到系统权限后，上传和执行了病毒，病毒类型为 Buran 家族勒索病毒。各地各部门应根据以上情况，加强自查，严格控制网络访问策略，关闭 windows 远程桌面服务;自查是否存在“永恒之蓝”(MS17-010)漏洞，及时修复存在

的漏洞。请各地各部门参照勒索病毒防范指引，加强对勒索病毒的日常防范。

附件：勒索病毒防范指引

省政务服务数据管理局

2020 年 7 月　日

附件

勒索病毒防范指引

勒索病毒是一种新型电脑病毒，主要以邮件、程序木马、网页挂马的形式进行传播。这种病毒利用各种加密算法对文件进行加密，被感染者一般无法解密，必须拿到解密的私钥才有可能破解。具体防范措施如下:

一、避免使用过于简单的口令。登录口令尽量采用大小写字母、数字、特殊符号混用的组合方式，口令长度不少于8 位。同时添加限制登录失败次数的安全策略并定期更换登录口令。多台机器不要使用相同或类似的登录口令，避免出现“一台沦陷，全网瘫痪”的情况。

二、重要资料定期隔离备份。对重要的数据和文件定期进行非本地备份，可以将数据备份在不同的存储类型设备，如服务器、移动硬盘、光盘等。

三、及时修补系统漏洞。定期为服务器和办公电脑打补丁，定期进行木马病毒查杀和修复漏洞。关闭非必要的服务和端口，如 139、445、3389 等端口。

四、避免使用不安全的远程运维方式。不通过远程软件的方式登录单位内网进行运维，如确实需要远程运维，可通过安全可靠的 VPN 登录方式。

五、提高安全意识。加强安全意识培训，不随意点击陌生链接、来源不明的邮件附件、陌生人通过即时通讯软件发

送的文件，在点击或运行前进行安全扫描，从安全可信的渠道下载和安装软件。

六、加强安全防护。加强终端防护检测能力，部署具备检测已知和未知勒索病毒的杀毒软件，避免传统杀毒软件只能基于已知病毒进行检测的弊端。部署流量监测、阻断类设备或软件，提高监测预警、事中阻断、事后回溯的能力。同时，在防火墙、路由器、交换机等网络边界设备设置严格的访问控制策略，保证网络安全。

七、加强应急响应能力。一旦发现感染勒索病毒后，及时将情况向本地网信和网警部门通报，请求协助处理；隔离感染主机，进行物理隔离和访问控制；联系专业的安全公司进行病毒查杀，修补漏洞。