针对勒索病毒预防排查的建议

针对勒索病毒频发，建议各部门对防火墙、杀毒软件等网络安全设备防护策略进行梳理和检查。

一、防火墙设备

1、检查防火墙规则库、特征库等是否为最新版本。

2、检查对外端口映射是否包含高危端口（如137、138、3389、445、22等），以及非必要的业务端口（如数据库端口）。

3、检查安全策略配置是否全面，防护区域、防护目标以及日志记录是否开启。

4、应用控制策略，建议针对业务规则设置为最小服务单元，针对重要业务系统的应用控制策略开启日志记录。

二、杀毒软件

1、检查业务服务器上是否部署杀毒软件，以及运行是否正常。

2、检查防护策略是否设置得合理，是否开启文件实时防护、Webshell检测、暴力破解检测和无文件攻击等。

如发生安全事件及时上报，安排协助排查。