勒索病毒防范指南

● 适用声明

本指南由 91 数据恢复团队原创，适用于企业日常预防勒索病毒攻击的安全防范措施。
阅读对象为:
企业 IT 部门负责人、安全管理员、系统管理员、数据库管理员、网络管理员。

● 系统安全防范措施

1．多台机器，不要使用相同的账号和口令，以免出现“一台沦陷，全网瘫痪”的惨状；

2．服务器及数据库的登录口令都要有足够的长度和复杂性，更改使用复杂密码，字母大小写，数字及符号组合的密码，不低于 15 位字符，并定期更换登录口令；

3．严格控制共享文件夹权限，在需要共享数据的部分，尽可能的多采取云协作的方式。

4．日常及时修补系统漏洞，同时不要忽略各种常用服务的安全补丁，并且开启自动更新功能。

5．关闭非必要的服务和端口如 135、139、445、3389 等高危端口，尽量不开放外网端口。

6、不开启使用系统自带的远程协助服务，使用其它远程管理软件，例如：TeamViewer，禁止员工电脑使用外网远程连接软件（禁止远程软件相关端口），如需使用，请通过 VPN 方式连接。

7、如果不需要远程桌面，就禁用远程桌面服务功能，如果必须要用远程桌面服务，务必更改掉系统默认的 Administrator 用户名， 并 3389 端口换成 33899 或者其他。禁用 GUEST 来宾帐户。

8、外网服务器不要有访问及修改任何内网计算机文件夹的权限；

9、安装专业杀毒软件，如果是安装 360 安全卫士，务必安装正式版【别用 Bate 版和极速版】，并开启 360 防勒索服务功能和防黑模式。必需设置杀毒软件软件退出或更改需要密码，防止黑客进入立即关闭杀毒软件。

10、备份、备份、备份！重要资料一定要定期隔离备份。进行 RAID 备份、多机异地备份、混合云备份，对于涉及到机密或重要的文件建议选择多种方式来备份，备份的文件建议放在 Linux 架构的服务器上，如是云服务器，一定要做好快照；

11、要求员工提高安全意识，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，尽量从安全可信的渠道下载和安装软件；

12、安装专业的安全防护软件并确保安全监控正常开启并运行，及时对安全软件的病毒库进行更新。

91数据恢复