探究事业单位计算机网络安全维护管理

事业单位计算机网络管理则是指对计算机病毒开展排查、预防，强化事业单位计算机网络管理安全性，积极构建安全防火墙，有效提升计算机应用技术水平和及时对电脑硬件、软件开展技术升级等。

2 计算机网络安全相关影响因素

2.1 网络开放性

网络具备开放性特征，无论哪一位用户均可参与到网络中来。再加上伴随信息技术的飞速发展，通过网络对单位、个人等信息进行获取变得更为容易。就好比，网络中开展人肉搜索，经由全体网民的参与，即可得到任何自身得到的信息，这已然与现实社会直接关联。

2.2 网络资源共享性

网络资源共享性属于计算机网络运行的一大特征，基于资源共享方可达成部门与部门相互间的有效联络，进而改善工作效率。然而也正是由于网络资源共享性，才为不法人员攻击单位计算机网络带来了可乘之机，只要单位内部信息资源许可外部服务请求，不法人员便可乘此机会对单位计算机网络开展攻击，进一步窃取单位内部信息。

2.3 网络操作系统漏洞

网络操作系统是达成网络信息传输运行的重要形式，经由硬件、软件系统操作，可开展各式各样网络行为。然而，受网络协议存在复杂性特征影响，使得网络操作系统操作期间往往会伴有各种漏洞，为计算机网络带来安全隐患。

2.4 网络系统设计弊端

网络设计指的是拓扑结构设计、一系列网络设备选取等。网络操作系统、网

络设备以及网络协议等均会或多或少造成相应安全隐患。科学合理的网络设计，不仅能够起到节约资源的作用，还可确保一定的安全性;不合理的网络设计则会带来不堪想象的网络安全威胁。

2.5 恶意攻击

一直以来，恶意攻击均属于计算机网络面临的一大安全问题，不法人员利用先进技术手段、木马病毒等方式对单位内部计算机网络进行侵袭，进一步恶意篡改、窃取单位内部信息，使得单位遭受极大损失。该种不法人员恶意攻击的行为，伴随黑客水平的不断提高，其入侵成功率也越来越高，一般事业单位通常难以做出有效防范。

3 事业单位计算机网络安全维护管理策略

全面事业单位计算机网络安全维护管理在时代发展新形势下，要紧随时代发展潮流，强化改革创新，在先进理念、成功发展经验的支持下逐步强化计算机网络安全维护管理，如何进一步促进事业单位计算机网络安全有序运行可以从以下相关策略着手：

3.1 强化计算机网络与信息安全工作

(1)在事业单位职工大会上，及时对上级发布的网络、信息安全工作文件精神进行传达，深入增强安全观念，提高安全意识。积极树立信息安全、人人有责理念，强化计算机安全管理水平及网络信息安全意识。对事业单位内部各项计算机网络管理制度予以完善，包括信息系统安全运维管理办法、计算机设备管理办法等，构建起明确到第一责任人的安全管理责任制度，并制定计算机网络安全管理细则，开展安全责任层级管理，积极促进网络及信息安全责任的有效落实。

(2)依据现阶段实行的标准化试点工作及绩效评定相关标准，对计算机网络

安全制度建设予以规范健全。对管理、操作予以有效规范，实现内外网识别标签的全面统一，于内外网设备、接口关键位置进行逐一张贴，防止由于误插网络而引发的违规外联。切忌于内网网络上接入相关无线设备，防止内网及其终端出现违规外联行为。

(3)强化事业单位计算机网络日常管理，增强日常宣传及计算机网络安全检测，提高职工计算机网络安全防范意识。不定期组织专业人员对计算机网络管理开展安全检测，实时监控计算机网络运行状况，及时对系统补丁进行升级，提高对恶意攻击的防御力，对计算机网络运行中存在的安全问题做出及时反应，积极促进计算机网络安全有序运行。

3.2 有序引入及更新网络应用技术

事业单位应主动积极引入一系列先进网络应用技术，诸如防火墙技术、信息加密技术以及防病毒技术等。要想开展好计算机网络安全维护管理，可一并选取网络版病毒防护软件、单机版病毒防护软件，前者安装于工作站上，后者安装于每一计算机单机上，为远程扫描数据资源带来便利的同时，改善病毒清除成效及系统检测成效。除此之外，条件允许的事业单位可引入生物识别技术，该项技术涵盖了人类指纹、面部、骨架等人体特征，即为强化版的安全识别方式。

3.3 强化计算机硬件技术维护管理

报警系统、线路截获、电源故障等一系列计算机硬件系统故障的引发均会对计算机网络安全造成一定影响，鉴于此，应当加大计算机硬件日常维护管理力度，事业单位计算机硬件技术维护管理可推行主动维护管理方式，该种方式是以月份、季度、年份为基础而推行的计划性检修，通过委派专业维护人员，以对事业单位计算机硬件开展维护管理活动。与此同时，切实依据信息安全等级保护相关

要求，对操作人员计算机、应用软件开展不定期风险评估，推行实时动态管理;加大对信息系统重要信息数据的安全管理力度，并定期予以安全备份，为数据提供切实安全保障。

3.4 强化计算机网络实时监测

网络监测指的是对网络对象安全程度开展信息反馈、信息监控，只要网络中出现数据传输情况，便可借助入侵检测、数据挖掘等一系列手段对数据是否正常开展评定，进一步得出存在异常数据流、不良数据流与否的结果。除此之外，还可应用相关安全防范技术将异常数据流、不良数据流朝伪主机、伪服务器上引导，尽可能确保计算机网络安全有序运行。

3.5 构建安全性控制的恢复、备份机制

安全性控制指的是在连接每一网络服务设备后对应推行的安全保障策略，可实现对相关不合理控制的有效限制。构建安全性控制的恢复、备份机制，可有效杜绝引发重要数据误删、重要数据遭受恶意篡改等情况。值得一提的是，即便该项机制可收获一定的成效，然而操作相符复杂，且依旧存在相应漏洞，有待后续对其开展逐步完善，提高成功率。

4 结束语

总而言之，计算机网络是一个极为复杂的系统，其有着十分强大的功能，然而在为人们生活、工作创造便利的同时，还会带来一系列安全风险。倘若网络信息遭受篡改或者窃取，势必会使事业单位遭受极大损失。鉴于此，相关人员务必要不断钻研研究、总结经验，清楚认识事业单位计算机网络维护管理内涵，全面分析计算机网络安全相关影响因素，开展好事业单位计算机网络安全维护管理，“强化计算机网络与信息安全工作”、“有序引入及更新网络应用技术”、“强

化计算机硬件技术维护管理”、“强化计算机网络实时监测”、“构建安全性控制的恢复、备份机制”等，积极促进事业单位计算机网络安全有序运行。