机关事业单位计算机网络安全防护探析

郝　瑞
北方实验室（沈阳）股份有限公司广州分公司　广东　广州　510000

摘　要：随着信息技术在机关事业单位广泛应用，计算机网络安全愈发重要。本文深入剖析了机关事业单位计算机网络面临的诸多安全威胁，涵盖网络攻击、数据泄露、网络漏洞以及移动设备接入安全问题等方面。同时，针对性地提出了相应防护措施，包括网络安全技术应用、安全管理制度建设以及人员安全意识培养等内容。旨在助力机关事业单位构建完善的网络安全防护体系，保障其网络安全稳定运行，确保政务工作顺利开展与信息资产安全。

关键词：机关事业单位；计算机；网络安全；防护探析

引言：在当今数字化快速发展的时代，机关事业单位的日常办公、政务处理等诸多工作都高度依赖计算机网络。其网络承载着大量敏感政务信息与关键业务数据，网络安全与否直接关系到单位职能履行、公共服务质量以及社会稳定。然而，当前网络环境复杂多变，机关事业单位计算机网络面临着来自黑客攻击、数据泄露等多方面的安全威胁，亟待加强安全防护。因此，深入探析机关事业单位计算机网络安全防护问题具有重要的现实意义。

1 机关事业单位计算机网络安全的重要性

机关事业单位计算机网络安全具有多维度的重要性。在信息时代，其网络存储与处理大量政务信息、公民数据等关键内容，如人口信息、财政数据等，网络安全是保障这些信息完整性与准确性的关键，避免数据被恶意篡改或损坏，从而确保决策依据的可靠，为科学施政提供有力支撑。关乎公共服务的连续性与稳定性。众多面向公众的服务如社保办理、税务征收等依赖网络平台，一旦遭受攻击导致网络瘫痪，服务将被迫中断，影响民众正常生活，损害政府公信力。涉及国家安全与社会稳定。机关事业单位在维护国家秩序、保障社会安全方面承担重要职责，其网络若被攻破，可能导致敏感的国家安全信息泄露，为不法分子或境外势力所利用，进而引发社会恐慌与混乱，威胁国家主权与社会和谐发展[1]。

2 机关事业单位计算机网络面临的安全威胁

2.1 网络攻击

2.1.1 黑客攻击

黑客攻击严重威胁机关事业单位网络安全。他们运用专业技术扫描网络漏洞，以此为突破口非法入侵。入侵后，可能肆意篡改政务数据，造成信息混乱；删除关键文件，破坏业务进程；窃取敏感信息，如机密文件与公民隐私数据，用于非法牟利或恶意目的，甚至发动DDoS 攻击，使服务器瘫痪，网络服务中断，极大地影响单位运行与公共服务提供，损害政府公信力。

2.1.2 恶意软件攻击

恶意软件攻击给机关事业单位带来诸多困扰。病毒可自我复制，如 Worm 病毒能迅速在网络中扩散，大量占用系统资源，让计算机运行缓慢甚至死机。木马程序善于隐藏，悄然窃取账号密码、机密资料等信息。蠕虫则自动传播，导致网络拥堵，使正常的数据传输和业务办理受阻，影响工作效率，破坏网络稳定，危及单位信息资产安全与业务的正常开展。

2.2 数据泄露

2.2.1 内部人员违规操作

内部人员违规操作是机关事业单位数据泄露的重要隐患。部分员工因安全意识薄弱，可能为图方便私自将单位机密数据拷贝至外部存储设备带出单位。或者在未经授权的情况下访问敏感信息系统并下载数据，甚至随意在不安全网络环境中处理工作事务。这些行为都可能使重要政务数据、公民信息等脱离安全管控范围，为数据泄露埋下祸根，严重威胁单位信息安全与社会稳定。

2.2.2 外部网络入侵导致数据窃取

外部网络入侵引发的数据窃取对机关事业单位危害巨大。黑客凭借先进技术突破网络防护，将目标锁定在存储于单位服务器中的海量数据，如政务决策文件、公民社保信息等。一旦成功入侵，他们便能窃取这些敏感数据，在地下交易市场售卖以获取高额利润。这不仅严重侵犯公民隐私权益，还可能使政务工作陷入被动，引发社会信任危机，对单位形象与国家信息安全造成难以估量的损害。

2.3 网络漏洞

2.3.1 操作系统漏洞

操作系统漏洞使机关事业单位网络暴露于风险之

中。如 Windows 系统曾出现的高危漏洞，可被黑客利用进行远程代码执行。由于操作系统广泛应用且基础，其漏洞影响范围大。若未及时更新补丁，黑客便能轻易绕过常规安全机制，获取系统权限，进而控制计算机、窃取敏感信息或植入恶意软件，对单位网络安全构成严重威胁，可能导致大面积系统瘫痪与数据泄露事件发生。

2.3.2 应用程序漏洞

应用程序漏洞在机关事业单位网络中也不容小觑。各类办公软件和业务应用系统在开发过程中难免存在缺陷。例如某些电子政务系统的 SQL 注入漏洞，攻击者可借此篡改数据库内容、获取用户信息。跨站脚本漏洞则能让恶意脚本在用户浏览器中执行，窃取登录凭证等敏感数据。这些漏洞一旦被利用，会破坏应用程序正常运行，使单位业务中断，同时危及数据安全与用户隐私。

2.4 移动设备接入安全问题

2.4.1 智能手机和平板电脑的安全风险

智能手机和平板电脑在机关事业单位网络应用中存在诸多安全风险。其便携性导致易丢失或被盗，一旦落入不法分子手中，设备中存储的单位内部应用数据、登录凭证等信息可能被窃取。而且，员工可能随意下载来源不明的应用程序，部分恶意应用会暗中收集设备信息，包括单位相关数据，并发送给第三方。另外，在连接公共 Wi-Fi 时，若未采取安全措施，网络通信易被监听，黑客可借此获取设备传输的敏感信息，从而威胁机关事业单位网络安全与信息保密工作。

2.4.2 移动存储设备的安全隐患

移动存储设备给机关事业单位网络带来显著安全隐患。U 盘、移动硬盘等在单位内使用频繁，若在外部不安全环境中使用后接入单位内部计算机，可能已感染病毒、木马等恶意软件。这些恶意程序会自动在内部网络传播，感染其他设备，导致系统故障、数据丢失或泄露。例如，一个携带病毒的 U 盘插入办公电脑后，病毒可能迅速扩散至整个局域网，破坏重要文件，瘫痪业务系统，使单位遭受巨大损失并影响正常工作秩序[2]。

3 机关事业单位计算机网络安全防护措施

3.1 网络安全技术应用

3.1.1 防火墙技术

防火墙技术是机关事业单位网络安全的关键防线。它依据预设的安全策略，对网络流量进行精准监测与管控。通过限制外部网络对内部网络的访问，仅允许特定的 IP 地址、端口和协议通行，有效阻挡黑客攻击与恶意流量。例如，可阻止未经授权的外部设备连接内部网络服务器，防火墙能够防止内部网络用户访问危险的外部网站，避免恶意软件的下载。它还能对网络数据进行过滤，筛选出潜在的安全威胁，为机关事业单位网络营造安全稳定的运行环境，保障信息资产安全。

3.1.2 入侵检测与防御系统（IDS/IPS）

入侵检测与防御系统（IDS/IPS）在机关事业单位网络安全防护中发挥着重要作用。IDS 能够实时监测网络中的各类活动，深度分析网络数据包，精准识别异常流量模式、恶意扫描以及可疑的入侵行为。一旦发现潜在威胁，它会迅速发出警报，通知管理员及时处理。IPS 则更进一步，不仅能检测，还能主动采取防御措施。当检测到入侵时，IPS 可立即阻断攻击源的连接，阻止恶意数据包进入内部网络，有效应对诸如 DDoS 攻击、SQL 注入攻击等多种网络威胁，确保网络的正常运行与数据安全。

3.1.3 数据加密技术

数据加密技术为机关事业单位的数据安全提供了坚实保障。对于存储在计算机硬盘、服务器以及传输于网络中的敏感信息，如政务机密文件、公民个人隐私数据等，通过加密算法将其转换为密文形式。即使数据被非法获取，若没有对应的解密密钥，攻击者也无法解读其内容。在存储方面，全盘加密可防止硬盘丢失或被盗后数据泄露。在传输过程中，采用 SSL/TLS 等加密协议，确保数据在网络传输时的保密性、完整性与真实性。

3.1.4 虚拟专用网络（VPN）技术

虚拟专用网络（VPN）技术对机关事业单位意义重大。它能够在公用网络基础上构建安全的专用通道，实现远程办公人员或分支机构与总部网络的安全连接。例如，员工在外出差时，借助 VPN 可如同身处单位内部局域网般访问内部资源，进行文件传输、系统操作等工作，且传输的数据都经过加密处理，有效防止信息在公共网络中被窃取或篡改。VPN 技术不仅保障了远程办公的安全性与便利性，还确保了单位网络边界的完整性，为机关事业单位拓展业务范围、提升工作效率提供了可靠的网络安全支持。

3.2 安全管理制度建设

3.2.1 网络安全责任制度

网络安全责任制度是机关事业单位网络安全管理的基石。明确单位主要领导为首要责任人，对整体网络安全负总责，各部门负责人承担本部门相关责任，将责任细化至个人岗位。通过这种分层负责机制，确保网络安全工作事事有人管。例如，在信息系统升级时，技术部门需保障操作合规安全；业务部门则对员工数据使用规范监督，将网络安全纳入绩效考核，对失职行为严肃

问责，促使全体人员积极参与维护网络安全，形成全方位、多层次的责任体系，保障单位网络环境稳定可靠。

3.2.2 访问控制制度

访问控制制度是机关事业单位网络安全的重要管控手段。依据员工岗位职能与业务需求，精细划分网络访问权限。普通员工仅能访问其工作必需的特定系统与数据，如财务人员可访问财务系统，而无法涉足人事档案库。采用多因素身份认证，如密码加指纹识别等，增强用户身份识别准确性。定期审查权限，员工岗位变动或离职时及时调整或收回权限。

3.2.3 数据安全管理制度

数据安全管理制度为机关事业单位数据资产保驾护航。首先对数据进行分类分级，如政务机密数据、普通业务数据等，针对不同级别制定差异化安全策略。对于机密数据采用更严格的加密存储与传输方式。建立完善的数据备份与恢复机制，定期在异地存储备份数据，预防数据丢失或损坏。规范数据生命周期各环节，从收集、存储到销毁都有章可循。

3.2.4 应急响应制度

应急响应制度是机关事业单位应对网络安全突发事件的关键保障。该制度详细规划了安全事件的分类标准，如网络攻击、数据泄露等不同类型。一旦发生事件，明确规定了报告流程，确保信息能迅速传达至相关部门，制定了针对性的应急处置措施，包括隔离受影响系统、收集证据等操作，以防止事件扩大。在事件处理后，还有完善的恢复流程，保障业务系统尽快重回正常运行状态。

3.3 人员安全意识培养

3.3.1 网络安全培训体系建设

机关事业单位应构建完善的网络安全培训体系。培训内容应涵盖多方面，包括网络安全基础知识，如网络架构、常见安全术语等，使员工具备基本的安全认知；网络攻击与防范手段，详细介绍黑客攻击原理及对应的防范策略，如识别钓鱼邮件、防范恶意软件入侵等；数据安全保护意识，强调数据的重要性及员工在日常工作中对数据保护的责任与方法。培训方式可多样化，采用定期集中授课，邀请专家深入讲解；开展线上课程学习，方便员工自主安排时间提升知识水平；组织模拟演练，模拟网络安全事件场景，让员工在实践中锻炼应急处理能力，从而全面提升员工的网络安全素养，为单位网络安全筑牢人员防线。

3.3.2 安全意识宣传活动

安全意识宣传活动在机关事业单位网络安全防护中不可或缺。可制作内容丰富的网络安全宣传手册，涵盖网络安全政策法规、安全操作指南、案例警示等内容，发放给员工随时翻阅学习。设计精美的海报张贴于单位办公区域显眼位置，以简洁明了的图文提醒员工注意网络安全风险，如谨慎使用公共 Wi-Fi、避免随意下载不明软件等。制作生动有趣的宣传视频，在单位内部会议、培训间隙播放，通过真实案例演示网络安全事故的严重后果，增强员工的直观感受[3]。

结束语

在数字化浪潮的席卷下，机关事业单位计算机网络安全防护工作任重道远。通过对网络安全威胁的深入剖析以及防护措施的全面探讨，我们明确了构建多维度防护体系的重要性与紧迫性。从先进技术的应用到完善制度的建立，再到人员安全意识的提升，每一个环节都紧密相扣。唯有持续强化网络安全防护，机关事业单位才能在保障信息资产安全的基础上，高效地履行公共服务职能，为社会稳定与发展提供坚实可靠的数字化支撑，从容应对未来网络安全领域的诸多挑战。

参考文献

[1]张彭.浅谈机关事业单位计算机网络安全与管理[J].电脑迷,2019,(04)：176-177

[2]陈滔文.政府事业单位信息化网络安全的实现[J].数字技术与应用,2019,(02)：193-194

[3]姚薇敏.浅析事业单位计算机网络安全维护管理[J].计算机产品与流通,2019,(12)：35-36