事业单位计算机网络安全防护技术分析

王婷婷 王喜华 张 璐 王经纬
（国网河南省电力公司南阳供电公司，河南 南阳 473000）

摘要：随着计算机技术的高速发展，使人们的生活和工作应用的频率更高，也相继出现了计算机安全问题。然而，在实际上事业单位的计算机网络运行过程中，仍然存在着较多的安全隐患和漏洞，这些问题会导致整个系统的崩溃，同时还会影响单位工作人员的正常工作，甚至会造成隐私信息的泄露。基于此，文章对事业单位计算机网络安全防护技术展开分析和研究，阐述了计算机网络安全的内涵，分析出事业单位计算机网络安全防护的重要性，探索出事业单位计算机网络安全现状和存在的隐患，并对网络安全的主要内容进行剖析，在此基础上提出了事业单位计算机网络安全防护策略，以供参考。

关键词：事业单位；计算机网络；安全防护技术

在科学技术高速发展的今天，计算机网络系统应用于事业单位，能够在一定程度上提高工作效率。正是由于如此，计算机网络在机关事业单位的日常工作中起到了重要的作用。然而，由于事业单位对于计算机系统信息储存的要求较高。在这种情况下，应加强安全性建设，避免出现更多的网络信息安全问题。在现阶段，对事业单位的计算机网络系统运行过程进行分析，有利于更好地开展其他工作，提升计算机的安全性，并提高事业单位的服务效率。

一、计算机网络安全的内涵

计算机网络一般是由一系列网络硬件设施和传输媒介组成的，它涉及到信息管理软件等要素。若要保障其工作的安全性，则需要注重硬件的安全网络传输介质的安全。为计算机网络硬件和软件建立和采用技术管理的安全保护，确保计算机网络的软件和硬件数据不被破坏核泄漏。然而，在实际上若要界定计算机网络安全的内容，就需要采用多种安全防护技术，确保各环节数据的安全性和完整性，保障其有效性，避免出现入侵和病毒木马造成的数据损害问题发生，保障计算机网络用户的信息安全。

二、事业单位计算机网络安全防护的重要性

在科学技术高速发展的背景下，事业单位计算机网络安全防护十分关键，重要性如下：

（一）保障事业单位正常运行

随着现代信息技术的高速发展，事业单位的工作与计算机和网络具有密切的联系。在新时代的背景下，事业单位会利用网络储存和收集信息，从而做好信息的有效识别。如果计算及内部网络系统遇到侵袭，则会出现信息安全的丢失，这也不利于机关事业单位工作的有效开展，容易导致信息系统的故障，不利于基础性工作的开展。如果计算机的网络安全遭遇到破坏，不仅无法使企业正常开展工作，甚至会出现个人信息的泄露问题。而提升网络基础数据的安全性，有助于更好地维持事业单位的正常工作运行，并利用网络基础设施信息系统开展相关的工作。

（二）保证事业单位信息安全

事业单位一般会参与到国家社会公共事务的组织和协调之中，履行公共服务方面的职能。然而，事业单位的性质也决定了它具有较强的保密性，同样也是维护信息安全的重要渠道，有助于保障我国事业单位信息安全的内在需求。事业单位对于个人信息的网络安全性能具有技术要求，面对个人信息的泄露和丢失问题，计算机网络安全系统应第一时间做出数据信息处理，尽可能地降低技术损失。而这些与专用计算机行业网络安全相关。只有保障机关事业单位个人信息的安全，才能更好地发挥互联网的重要价值，做好相应的管理和规划。

三、事业单位计算机网络安全现状和存在的隐患

（一）网络安全现状

我国互联网的起步相对较晚，但其发展速度比较快，网络安全的法规并不完善，并且有部分领域处于真空的状态之中。网络操作监督不到位，存在更多的安全隐患。从我国现阶段的机关事业单位网络安全状况看，主要存在以下几个特点：

第一，网络安全设施薄弱。有部分机关事业单位在网络安全防护领域并没有硬件设置资源，即使有也是一些基本的设施，遇到如果遇到网络攻击时，难以进行防护。大部分机关事业单位只能利用软件达到防护的目的，并且使用的软件质量具有较大的差异性，这也会在某种程度上给事业单位的网络安全带来消极影响。

第二，网络安全管理制度欠缺。大部分行业行政单位并没有建立科学完善的网络安全管理制度，并且很多制度的标准化不足，没能有效执行管理制度，这也导致在制定安全策略的过程中，缺乏安全指导。

第三，网络安全意识不强。很多机关和事业单位对于网络安全的重视性不足，并且领导层的网络安全意识淡薄，没能认识到网络安全的重要性。很多普通职工的责任感并不强，无法积极投入到网络安全管理局工作中，并且缺乏专业的网络安全管理人员，难以实现科学有效的管理。

（二）存在的安全隐患

在科技信息高速发展的背景下，人们的计算机应用频率更高。然而，随之相继出现了计算机安全问题。在实际上事业单位的计算机网络运行过程中，仍然存在着较多的安全隐患和漏洞，威胁机关事业单位的安全隐患比较多，主要有以下两方面：

第一，网络安全隐患来自机关事业单位的内部，主要是人为主动的安全隐患和非人为被动的安全隐患。人为的安全隐患是由于员工大意，可能是个人利益处理公务，也可能是有预谋的破坏，如果出现安全隐患，则会直接带来更多的危害。因为这些潜在的安全隐患是反入侵防御系统无法检测的。非人为被动的安全隐患可能是因为员工的大意，有可能也是因为个人利益问题，通常出现安全隐患，是反入侵防御系统难以检测和防范的。非人为被动的安全权利隐患主要包括单位缺少信息安全管理体制，并且有部分员工的安全责任意识不足，缺乏信息安全信息技术，这些问题都会对机关事业单位的网络信息安全造成相应的威胁。

第二，来自网络的隐患。一般情况下机关事业单位的网络是与互联网连接的，这样能够为员工的工作提供便利。常见的网络安全隐患包括病毒、木马和黑客攻击等，这些问题会直接给机关事业单位造成影响。严重时甚至会给机关单位和人民的生产生活带来实质性的影响。与此同时，互联网技术的不成熟可能也会被非法分子加以利用，并直接对机关事业单位带来危害。

四、网络安全的主要内容

第一，是网络安全体系。组建计算机网络的目的是有效处理

各类具有价值的信息，并利用计算机搭造相应的通信平台。网络安全体系主要包括安全模型和计算系统、网络安全风险评估等内容，重点是根据网络安全威胁因素，确定网络资产，并进行资源的调配，了解其后果，根据安全模型设计和开放网络安全产品。网络安全体系建设的核心内容是网络安全管理，涉及到安全评估标准和方法，从而更好地制定安全措施。

第二，系统安全平台。系统的安全一般涉及到网络的物理安全和安全操作体系等。操作系统主要包括基本的操作系统和配置的安全性，更好地实现数据修复，保障数据库系统的安全性。

第三，网络攻击与安全防护。互联网的基础是 TCP/IP 协议，它一般是指网络互联设备，并加强联网能力操作系统建设。TCP/IP 存在一定的漏洞问题，如果是最新的版本同样也存在。漏洞的出现与网络的安全性之间具有密切的联系。如果不知道系统是如何进行攻击的，再好的防御都无法承受住考验。如果没有防御的能力，网络的安全性同样也会受到影响，不利于网络的稳定运行，甚至会造成各类经济损失的问题，影响到社会的安全。在网络安全防控的过程中，应做好安全性防护，充分做好网络安全的审计工作。

第四，密码技术应用。密码学有助于为数据提供机密性，并呈现出更加完整的数据信息。在大多数情况下，数据加密是保证数据机密性的重要方式。一个加密网络不仅可以避免非授权用户的窃听，还能够更好地防范恶意代码。

第五，网络安全应用。网络安全应用的内容相对较为广泛，涉及到网络层和虚拟网络安全的有关信息，并且与 Web 安全技术具有密切的联系。

五、事业单位计算机网络安全防护策略

在信息时代背景下，人们的生活和工作应用计算机的频率逐渐提高，也相继出现了计算机安全问题。然而，在实际上事业单位的计算机网络运行过程中，仍然存在着较多的安全隐患和漏洞，这些问题会导致整个系统的崩溃，同时还会影响单位工作人员的正常工作，甚至会造成隐私信息的泄露。为了避免计算机网络安全使用过程中存在的安全隐患，并将其服务于机关事业单位之中，则需要提高计算机网络的安全防护性能，做好对安全防护技术的研究和应用。因此，事业单位计算机网络安全防护应从以下几方面出发，做好相应的工作，提升机关事业单位的服务质量：

（一）加强对网络安全人员的培养

网络安全的构建离不开技术人员的共同参与，网络安全技术管理人员的专业技术素质水平高低同样也会直接影响整个事业单位信息网络的安全和可靠性。因此，这就需要网络安全技术人员提高自身的素质能力，定期组织相关的安全技术工作者参与到网络安全知识讲座之中，提升专业人员的技术能力。除此之外，单位部门的多名专业安全技术人员在经过统一的培训后，也被认可在整个单位中及时开展对其他岗位员工的管理知识培训，从而提升员工的管理能力。只有营造良好的人才培养环境，才能让在职员工形成良好的网络知识素养。

（二）建立网络安全规范制度

计算机网络安全故障的技术性因素比较关键。然而，一些制度性因素同样不能忽视。单位计算机网络的安全维护不能脱离网络规范和制度，这就需要保证其执行力。因此，行政单位应做好企业网络安全管理工作，确保工作的安全性和可靠性。与此同时，这也是各级机关单位和组织开展安全管理工作的核心因素。而各单位部门应设定相应的信息安全管理科室，在保障网络信息的安全的同时，根据上级领导和技术人员自身的工作职责，设定相应的规范制度，发挥出监督的重要作用。与此同时，科室人员参与到网络监督工作中，才能保障网络安全信息管理的有效性。

（三）强化网络安全技术革新

在实际上若要界定计算机网络安全的内容，就需要采用多种安全防护技术，确保各环节数据的安全性和完整性。

首先，防火墙。防火墙是一种网络安全防护机制，它能够有效实现软件与硬件的结合。防火墙是一种过滤性的结构网，它能够基于网络安全的空间开展工作。因此，它的主要作用在于监控网络信息的特点，对未经授权的非法通信进行阻断，确保内部网络的安全性。

其次，入侵检测。入侵检测一般是以计算机网络信息的收集和分析为主，进一步发现网络和系统中存在的入侵性的安全措施。它使用异常监测技术，并通过加强监测，通过监测的不同结果进行安全性检验，尽可能地将入侵的安全风险降到最低。

再者，漏洞扫描。漏洞扫描是事业单位网络安全设置的重要组成，他通过本地计算机系统和网络系统的扫描，来进一步发现存在的问题和有可能被攻击的节点，达到对网络安全的有效监测。因此，相关的信息管理工作者应利用扫描结果做好漏洞上的修复，避免出现更多的问题，给出相应的预防方法。与防火墙的被动防御有所差异，漏洞扫描是一种主动性的防范形式，有助于实现与防火墙的密切配合，发挥出事半功倍的效能。

最后，加密技术和身份认证技术。机关事业单位内部机密性相对较高，其安全性也比较高。因此，事业单位在进行数据储存和传递的过程中，应充分利用各项加密技术，从而保障信息的真实性和安全性。一般而言，数字加密会以原始形式为核心，并利用相应的加密密钥将其变为密文，保障其安全性和可靠性，并保障传输的过程不被截取。通过加密机的有效应用，能够保障机关事业单位的网络安全。除此之外，通过身份认证技术保护单位的网络安全，并通过验证访问者的身份做好相应的授权判断。

（四）提高网络硬件和软件的安全性

若要更好地实现网络安全硬件设备的建设，则需要优化备份数据的服务器，构建硬件防火墙。不仅如此，应确保网络计算机操作系统的安全性，并利用以 Linux 为内核的国产自主知识产权操作机制，及时提取出其中的漏洞，保障系统的便捷与安全。不仅如此，在机关事业单位的网络安全结构体系中，所有的服务器和终端计算机都需要安装安全防护的软件，除了要安装单机版的防火墙之外，还需要部署网络防火墙软件。

六、结语

综上所述，计算机网络在机关事业单位的日常工作中起到了重要的作用，在实际的工作中若要确保计算机网络始终处于安全的状态是不可能的。在大数据时代背景下，计算机技术会遇到全新的漏洞和病毒。对于机关事业单位的网络系统来讲，则需要更新自身的安全防护技术的同时，做好相应的安全管理，避免出现不安全的情况，呈现出一个更加安全可靠的网络环境。

参考文献：

[1] 赵云山，阮兴卫 . 行政事业单位计算机网络安全防护措施探讨 [J]. 科技视界，2021（30）：27-28.

[2] 高士平 . 机关事业单位计算机网络安全防护探析 [J]. 中国管理信息化，2020，23（22）：204-205.

[3] 李长智，孟超慧 . 信息化时代计算机网络安全防护技术的探讨 [J]. 电子世界，2020（14）：68-69.