计算机网络信息安全的有效防护对策

苏伟哲

（承德县应急管理局　河北　承德　067000）

[摘　要]目前，我国科学技术水平显著提升，在这样的背景下，计算机网络已经成为社会主流应用方案，走进了各行各业并得到充分应用。通过合理应用计算机网络，可以进一步拓展信息传播渠道，提高其整合效率，具有节约人力成本、提高工作质量的重要用途。但是，计算机网络信息应用普遍存在风险问题，若未采取可靠防护方案，便有可能导致负面问题产生，引发不必要的损失出现。本文探讨了计算机网络信息安全意义与核心内容，分析了计算机网络信息安全面临的主要问题，研究了计算机网络防护信息安全对策，以供参考。

[关键词]计算机；网络信息安全；防护对策

【DOI】10.12252/j.issn.2096-6288.2021.12.310

引言

科学技术的不断更新，已经让计算机网络融入人们生活中的方方面面。在这样的背景下，使用计算机已经成为人们离不开的一种生活方式。对于企业而言，如果离开了网络与计算机，那么维持日常运营将是无比艰难的。问题是，计算机网络技术给企业运行带来便利的同时，也在某些方面存在弊端，比如信息安全问题，如果处理不当，则可能造成大量信息外泄的情况，最终给企业带来难以弥补的伤害。因此，构建高效安全的计算机网络信息体系，确保企业的重要信息不会外泄，是一件重要且具有长远意义的事情，需要相关人员提高重视。

1.提升计算机网络信息安全的必要性分析

基于信息时代背景下，各种工作内容的开展都与计算机网络技术有着极为紧密的关联。分析得知，科学地对计算机技术加以利用，人们能够快速且便捷地对各种复杂数据信息加以处理，合理地进行收集和整合，高效地存储。并且，依托于计算机网络，借助其庞大性以及广泛性特征，可以不断对工作效率及质量进行提高，有利于社会经济效益的整体提升。同时，计算机网络的应用，还能保证信息的安全，可以更好地维护行业商业机密，让国家的重要信息内容得到良好保护。通常情况下，如果一些重要的信息数据被各种病毒所干扰或者受到外界因素的侵扰而遭到破坏，必然会影响到社会的稳定，对人们的生活以及国家发展造成了不利的影响。故而，全面促进计算机网络信息安全的提高，能够为社会及企业的发展做好全面准备。

2.计算机网络信息安全影响因素

2.1受人为因素的影响

计算机网络信息安全存在隐患也受到人为因素的影响。人为因素可以将其分为以下两类，第一类是部分软件编程人员为了后期维护工作更为便捷，通常会采用设置“后门”的方式对程序进行编撰，而这一编程方式极易被不法分子入侵，从而窃取所需要的信息，导致数据信息泄露，给人类生产生活带来严重的负面影响。另一类是用户在使用计算机网络系统时，由于自身安全防护意识薄弱，缺乏相应的计算机网络信息安全防护知识和技能，使用完毕以后未及时对其页面进行关闭，导致信息泄露，从而为个人、单位、国家发展带来诸多负面影响。此外，部分企事业单位并未对办公系统进行加密，任何人员都可以使用办公设备登录网络系统，加大了数据信息泄漏的风险性。

2.2计算机病毒

计算机病毒对于计算机网络信息安全的威胁巨大。不法分子通常以人为代码或者编写的各种程序对计算机内部数据进行破坏，从而窃取用户信息或者截取关键信息，对信息应用的主体实施敲诈勒索，给信息应用的主体带来了巨大的经济损失。计算机病毒的特点是传播速度极快，且传播范围较广，在极短的时间内对大量的计算机用户进行攻击。同时计算机病毒具有较强的隐蔽性，通常难以被主动发现，往往在产生破坏行为之后，才会被信息应用的主体发现，而此时造成的破坏，已经难以挽回。

2.3木马的侵害

木马在某些程度上，与计算机病毒是相似的。它是指在正常的程序中隐藏着一段可以对计算机造成不同程度破坏的代码。通常情况下，木马隐藏在一些图形软件或者是游戏里，如果没有经过特定的训练，普通人是很难发现的。换言之，用户会以为这是一个好的程序，于是着手使用，而程序中所包含的木马，就会攻击计算机系统，从而造成文件被破坏与删除。部分木马病毒甚至会让计算机硬盘格式化，使其里面所储存的文件全部消失。最为重要的是，这些木马可能会盗取计算机里面的重要内容，给企业的日常运行造成不可估量的伤害。

3.计算机网络防护信息安全对策研究

3.1计算机软硬件对策

（1）应用病毒防护与防火墙。计算机平台软硬件属于网络信息技术应用的基础架构，为尽可能提高安全级别，应当重视软硬件平台的防护对策部署，以确保相关体系具有健全特征，降低出现不良问题的概率。针对软件平台进行防护，可以通过安装病毒防护软件与防火墙软件等途径，强化计算机本地对于信息的保障力度。当前，病毒防护方案能够集成入侵检测、应用程序控制、启发式分析等多种先进技术。这些技术可以有效提高软件平台应用安全性，使网络信息传递能够在理想条件下执行，最大限度降低风险级别。除此之外，防火墙还可以部署硬件防护类型。硬件防火墙相对于软件能够承受较大的流量攻击，如DDOS等，有利于保障计算机网络应用可靠性，避免由于违规操作引发的瘫痪问题[5]。因此，需要重视软硬件防护对策的应用，确保相关负面因素能够得到排除，实现理想控制目标。（2）及时修补系统漏洞。漏洞属于计算机系统与网络系统不可避免的缺陷，其本质上与底层逻辑以及程序编写方式存在关联，无法预先解决。因

此，为降低漏洞对计算机网络信息产生的负面影响，应当采取漏洞同步修护策略，确保相关系统能够及时获取更新补丁，解决程序中存在的漏洞，避免受到针对性网络攻击。大部分网络信息攻击风险均需要利用潜在漏洞，使自身能够获得系统最高权限，进而执行破坏指令。通过设立相关条例规范漏洞更新，或定期检查漏洞情况，可以避免漏洞被不法分子所利用，损害计算机网络信息传递体系。因此，需要重视漏洞更新工作，确保系统能够在理想条件下运行，提高网络信息技术应用安全性。

3.2加强对加密技术的应用

首先，通过先进的技术，对网络数据库进行加密。当前许多企业由于缺乏对网络数据库的重视，在设置时，会将其设置为较低的级别，为计算机网络信息的安全埋下隐患，因此容易遭到不法分子的恶意袭击。想要改变这种状况，就需要对数据库进行加密，使相应的访问权限受到严密的限制，以此来保护机密信息的安全性。其次，对重要软件进行加密。部分杀毒软件在工作过程中，会使计算机感染病毒，从而给整个计算机系统造成不同程度的伤害。因此，在对数据进行加密时，需要对相对机密的数据文件进行科学的排查，看其是否感染上杀毒软件的病毒。如果有，那么立刻采取有效的方式，将病毒消灭。同时，在对数据加密时，还需要对杀毒软件进行加密处理，以便杀毒软件不会成为携带病毒的工具，从而给计算机系统造成不可估量的损害。最后，对VPN进行科学的加密。许多企业或者是企业在进行办公时，为了提高办公的效率，会使用模拟专用网络，从而在企业或者企业网络涉及的范围之内，都能实现数据的共享。部分跨区经营的企业，为了达到这个目标，还会建立广域网。不管是何种网络，计算机网络信息安全都应该是其最为重要的事情，为了达到这个目标，企业或者是企业等计算机网络信息构建者，可以通过对路由器访问的控制，来完成网络信息安全保护的目标，并在信息传输的过程中，通过有效的措施，对密钥进行科学地加密，以此来增加数据的安全性，确保计算机网络安全系统不会遭到侵入与破坏。

3.3采用网络隔离技术

采用网络隔离技术，能够最大程度地避免因操作不当而出现的信息泄露问题。在实践中，网络隔离技术可以通过物理办法的隔离来维护计算机网络信息的安全。在应用过程中建立安全通道隔离技术，借助相应的硬件设备和专有的安全协议，以及加密验证等多种方式实现网络隔离以及数据交换，通过这样的隔离防护，也能够最大程度地保护计算机网络的安全。与此同时，也应当增强网络安全准入控制的能力。在计算机网络信息安全维护的过程中，允许合法的端点接入公用网络。具体来说，在应用公用网络之前首先进行“申请”，通过系统排查之后，确定为安全网络才将这些网络转入公用系统中，从而保护计算机网络安全。

3.4定期使用杀毒软件对计算机网络环境加以清理

在使用计算机网络的时候，应该对杀毒软件进行有效利用，清理计算机网络系统，保证病毒能够在第一时间发现，然后及时地进行控制和处理，让人们可以更加放心地对计算机进行使用，让网络系统能够处于安全的状态，同时在计算机网络系统运行阶段，硬件设施所发挥的作用和价值非常大，而如果硬件出现了问题，必然会影响计算机系统的整体运行，甚至会导致计算机出现故障。对此，为了可以更好地改变这一现状，一定要结合具体情况，高效地管理计算机硬件，利用相对科学的方式对硬件设施加以维护。此外，需要定期地检查和更换计算机硬盘，确保相关数据信息能够更加完整安全，不会出现任何的问题。

3.5完善计算机网络信息系统安全管理机制和测评方案

人才作为计算机信息系统中的重要人员，其素质高度关系着计算机风险防御能力。因此，企事业单位负责人要完善计算机信息系统安全管理机制，可以通过引进专业人才等方式来提升计算机网络防御级别，利用一些专业理论、技术、经验等方式来提高网络安全管理级别，从而提高内部和外部网络交流的安全等级。当然，对于特殊的系统也可以采用第三方维护的方式对其进行解决，并利用科学化手段对其进行测评，比如金融行业、政府机关等，针对其系统中存在的隐患性问题进行测评并解决，降低数据信息泄漏的风险性，确保计算机信息系统稳健运行，更好地为人类社会发展服务。

3.6创设健全的计算机网络管理体制，强化网络管理安全性

（1）社会企业与协会等应当要积极创设健全的计算机网络系统安全管理体系，引入全新的网络信息安全防护方法来创设计算机技术平台，从而不断强化计算机网络系统运行的稳定性与安全性。（2）加强对计算机操作人员的规范化引导，企业一方面要积极倡导计算机操作人员开展自主学习，不断提升自身的网络素养，另一方面也要定期开展工作人员专业知识与技能培训活动，引导操作人员建立网络信息安全保护思维，提高计算机网络安全防护意识，能够全面了解与合理应用市面主流信息安全防护软件，进一步强化计算机数据信息的安全水平。（3）企业应当要结合自身实际应用环境引入数据认证技术，科学合理管控计算机网络的访问频率，同时依托于多种形式的计算机网络数字认证手段，进一步提高计算机内部网络运行的可靠性与安全性，有效避免网络信息被不良人员窃取与盗用等。

结语

综上所述，计算机网络信息技术应用阶段，安全性属于较为关键的发展任务之一。通过结合主要问题，部署实际应对方案，能够最大限度提高网络信息安全性，对未来进一步发展具有正面影响意义。

参考文献

[1]郑伟贞.关于计算机网络信息安全及其防护对策探析[J].电脑编程技巧与维护，2020（11）：163-165.

[2]王琛灿，徐杨斌，范乙戈，罗宇浩.计算机网络安全防御系统的实现及关键技术探析[J].网络安全技术与应用，2021（5）：20-22.

[3]周晶波.大数据时代计算机网络信息安全研究：评《网络安全态势感知：提取、理解和预测》[J].安全与环境学报，2021，21（3）：1388.

[4]杨佳.计算机网络信息管理及其安全防护策略[J].贵州农机化，2021（4）：47-48+51.

[5]陈富斌.关于计算机网络安全防范措施的思考[J].电脑与电信，2016（12）：84-85.