

计算机网络安全技术的影响因素与防范措施

贺云龙

(江西新能源科技职业学院, 江西 新余 338000)

摘要: 计算机网络技术的不断发展, 推动了我国社会经济的迅速发展。在计算机网络技术的影响下, 人们的工作和生活得到了极大的便利, 同时也增加了人们之间的交流。但是在计算机网络技术应用过程中, 出现了许多安全问题, 威胁到了人们的日常生活。为了解决这一问题, 必须要加强对计算机网络安全技术的研究, 进一步完善计算机网络安全技术应用体系。本文主要对计算机网络安全技术进行概述, 分析影响计算机网络安全因素, 并提出有效的防范措施, 希望能真正构建一个健康、和谐的计算机网络应用环境。

关键词: 计算机网络安全技术; 影响因素; 防范措施

随着我国科学技术的蓬勃发展, 计算机技术已经逐渐成为了人们生活中不可缺少的一部分, 它极大地方便了人们的日常生活, 也为工作、学习以及娱乐带来了诸多便利。在计算机技术为我们带来便利的同时, 一些安全问题同样不容忽视。计算机网络安全是一项非常复杂且综合性较强的工作, 要想保障计算机网络安全技术能够得到有效应用, 就需要结合当前计算机网络安全所面临的问题和影响因素进行深入分析与研究。因此, 如何加强计算机网络安全技术的研究和应用, 成为当前必须要重点考虑的问题之一。

一、计算机网络安全技术概述

随着计算机技术的不断发展, 计算机网络安全问题已经逐渐成为影响人们生活、工作以及学习的一个重要因素。在计算机网络安全技术发展过程中, 人们已经开始逐步将各种技术应用到计算机网络安全中, 这些技术主要包括了防火墙技术、访问控制技术以及数据加密技术等。防火墙是目前应用比较广泛的一种计算机网络安全技术, 其主要是通过对外部网络进行有效隔离, 从而实现为内部网络提供安全保障的目的。访问控制技术可以很好地实现对计算机用户的访问权限进行有效控制, 从而防止非法用户对计算机资源进行占用。数据加密技术主要是指通过对加密算法的不断改进和完善来实现对数据信息的保护。

信息安全已经成为影响国家发展的重要因素之一, 但是, 现如今, 我们还没有从系统上规划它, 在技术、政策以及产业方面也没有形成相对应的发展对策。鉴于计算机网络安全问题频发, 技术研发与风险防范体系构建仍旧是一项需要长期探索的任务, 不可掉以轻心。

二、计算机网络安全的影响因素

第一, 外界危险因素。在当前互联网高速发展过程中, 很多人为了获得更多利益, 会利用非法手段对计算机网络信息进行窃取, 这样会给用户带来严重的安全隐患。另外, 还可能存在一些黑客入侵计算机网络系统的现象, 这样也会给用户带来严重威胁。通常情况下, 黑客入侵计算机的技术手段多种多样, 尤其会重点攻击网络安全防范意识薄弱的计算机网络, 这样就很容易导致用户的资料信息出现泄露、丢失的现象, 甚至某些时候还会导致整个系统陷入瘫痪的状态中, 不仅仅对个人, 对国家也是重大的损失。

第二, 计算机病毒。计算机病毒作为一种破坏性极强的攻击形式, 对计算机网络系统的安全将造成严重威胁。它的传播速度

非常快, 并且不容易被删除, 计算机一旦感染上病毒, 那么它本身的功能就会遭到极大的破坏, 可能会出现信息丢失、数据被破坏等各种各样的严重问题。更严重的是, 如果计算机病毒自由传播, 那么它也有可能感染其他功能和系统, 与此同时, 病毒本身也会进行自我进化。由此看来, 计算机病毒是影响计算机网络安全的重要因素之一, 如果不能有效控制和处理, 会严重影响用户正常使用网络, 甚至造成巨大经济损失。

第三, 操作系统因素。操作系统在计算机系统中发挥着重要的作用, 对于计算机网络安全技术的研究具有重要意义。操作系统一旦出现故障, 就会影响信息系统的安全性能, 如果问题严重, 还会导致用户信息丢失或者是设备损坏。

第四, 监控手段不科学, 不合理。要想避免黑客入侵, 那么就需要构建科学有效的监控和评估体系, 这样就能准确且精准地判断整个网络是否安全, 即使出现问题也不必惊慌, 相关工作人员可以根据具体问题制定并实施有效的安全策略, 但是, 纵观现今如今的监控手段和监控体系, 依然存在着一系列的问题亟待解决。

三、计算机网络安全防范措施

(一) 增强安全意识, 系统规划网络

首先, 加强网络安全意识。目前, 计算机网络安全问题已经成为影响我国计算机网络运行质量的主要因素, 因此, 只有加强计算机网络安全意识, 才能从根本上解决计算机网络安全问题。在实际工作中, 相关人员应该对当前我国计算机网络存在的安全问题进行深入分析和研究, 从而确定哪些属于计算机网络安全问题。在具体实施过程中, 他们可以通过制定相应的防范措施来降低这些问题带来的诸多消极影响。比如, 为了保护信息数据安全, 可以将其存储在虚拟空间中, 通过虚拟空间达到数据保护的的目的。此外, 还可以通过对系统进行定期升级和维护来提升系统的安全性, 同时, 也可以采用一些防护技术来保护信息数据不被黑客利用和入侵。

其次, 合理规划网络。其一, 对计算机网络进行合理规划和设计。一方面, 在实际设计过程中要明确系统安全策略的目标和实现方法, 另一方面, 在制定安全策略的时候加强对防火墙技术、数据加密技术、病毒防治技术的应用。其二, 充分考虑计算机网络安全问题中存在的很多不确定因素, 采用多种安全手段来保障计算机网络安全。比如, 可以采用物理隔离技术、访问控制技术以及数据备份技术等来保障计算机网络安全。

此外, 还应该不断加强对软件安全漏洞的研究和分析。针对当前我国在软件方面存在的很多安全漏洞问题, 可以采取有效措施对软件进行漏洞检测, 以提高软件的安全性和可靠性; 通过对软件进行扫描来发现病毒木马等危害系统运行安全的因素; 通过对软件进行杀毒处理来防止病毒入侵计算机系统。

(二) 关注系统状态, 建立安全防线

计算机网络系统的安全问题, 不仅体现在计算机网络系统本身的安全, 还体现在计算机网络系统外部的安全。由于计算机网络系统与外部环境相互影响, 所以这就要求相关人员必须要加强对系统状态的关注, 建立完善的安全防线。一方面, 可以采取主动防御的方式来加强对计算机系统的保护。在使用网络资源时,

一定要遵循先使用、后付费的原则,提高计算机软件、硬件及操作系统的安全性。另外,也可以采用防火墙技术来保护计算机网络系统。防火墙技术主要是利用防火墙来保护网络数据信息,防止非法用户通过非法途径获取网络信息数据。在当前形势下,应该不断提高防火墙技术应用水平,建立更加完善、合理的安全防护机制。同时,还可以采用加密技术来对用户隐私进行保护,采用数字证书技术来提高用户身份认证的安全性。

加密技术。加密技术是一种非常有效地保护用户隐私的安全防护手段,不会泄露用户的个人隐私。目前,常用的加密技术主要分为两种,分别是对称密码和非对称密码。其中,对称密码技术主要是指将数据信息进行加密处理,通过算法来实现信息数据的安全保护,这种技术可以有效防止非法用户通过暴力破解的方式获取用户隐私信息。非对称密码技术主要是指在解密时需要使用与之相反的密钥,通过这种方式可以有效保护用户隐私信息。但是,非对称密码技术也存在一定缺陷,因为其在数据信息解密时需要使用到两个密钥,这样就会增加网络数据传输过程中的安全风险。但是,普遍看来,由于不同的加密技术采用的是不同算法和密钥进行加密处理,所以加密技术具有较高的安全性。

数字证书。数字证书主要是指能够对电子文档进行加密的一种信息技术,其主要原理是通过对信息进行加密,然后再向网络传输,以达到对数据信息进行保护的目的。由于数字证书技术具有较高的安全性,所以目前其已被广泛应用于计算机网络系统中,为其提供了更为安全的防护措施。一方面,数字证书能够在用户端和服务器端之间建立一道安全屏障,防止用户访问服务器时被篡改或窃取信息。另一方面,数字证书能够对用户身份进行识别,从而提高系统安全管理水平。另外,数字证书还能够对系统身份进行验证,保证网络资源的安全性。在数字证书技术中,主要包括加密、验证两种方式。其中,加密主要是指利用公钥对信息进行加密处理后传输;验证主要是指通过密钥对信息进行验证处理。

(三) 加强数据收集,保障网络安全

在计算机网络系统中,数据信息是非常重要的一项内容,也是保证计算机网络安全运行的重要组成部分。在实际工作中,我们要充分利用计算机网络数据信息来保证网络安全运行。在数据信息收集工作中要注意以下几个方面:

第一,加强对数据信息来源的检查与分析工作。在计算机网络系统中,数据信息往往是比较复杂的,因此,相关人员要及时对其进行检查与分析工作,避免出现错误信息以及无用信息,影响到计算机网络系统正常运行。

第二,加强对数据信息传输过程中传输路径方面传输内容的检查与分析工作,避免出现黑客或者病毒攻击等问题导致数据泄露以及一些恶意攻击等情况发生。在实际工作中要加强对用户所提供数据信息安全管理,同时也要加强对数据信息的审核工作和加密处理工作,从而提高计算机网络系统运行的安全性和可靠性。

第三,做好前期规划。数据安全是一项整体性的工程,在网络环境、应用、服务器、管理等各个环节都有可能引发安全问题,进而导致信息泄露。因此,在计算机网络系统构建前期,就应加强数据管理,尤其应对每个可能泄露信息的环节制定相应的防范措施,注意数据在各个环节的流转情况,结合数据保护的需要,针对不同类型的数据制定不同的安全策略以及控制措施,这样可以有效避免某些环节非法获取系统内的个人信息,进而保护数据和网络系统安全。

(四) 建设专业团队,加强风险管理

计算机网络安全维护一方面需要依赖软件、硬件以及先进技术的防御,另一方面离不开专业的网络评估以及监控人员。专业团队通常都是站在黑客的对立面,通过适时对网络进行监控与管理,观察网络是否存在被不法分子攻击的风险,在此基础上对计算机网络安全系数进行整体评估,针对问题提出针对性的改进建议,以便建立完善的网络运行机制。

专业团队建设,首先,注重加强对相关人员的培训,提高他们的综合素质,使他们掌握更多先进的信息安全技术知识与技能。其次,在专业团队中建立科学合理的评价机制,定期对工作人员进行考核,如果考核不合格则要及时更换。最后,对工作人员进行定期培训,增强他们的安全意识和风险管理能力。除此之外,加强计算机网络安全技术研究和应用需要大量资金与人才的支持,由此看来还要加强对这项研究工作的投入。通过政府支持、企业参与以及个人努力来共同建设一支优秀、专业的计算机网络安全技术研究与应用团队。

(五) 应用数字签名和身份认证技术

数字签名与身份认证技术主要是通过对电子信息进行加密来达到保护网络安全的目的,在这种情况下,只要用户使用了电子邮件、应用程序以及网页等,都会被网络服务器保存下来,同时还可以进行重放攻击与伪造攻击。因为只有计算机网络中的用户才能够接触到这些电子信息,所以在网络传输过程中很容易出现数据被篡改的情况。为了解决类似的问题,可以通过数字签名技术与身份认证技术来对数据进行加密。这两种技术都是在确认信息是否真实的基础上实现的,不需要用户进行确认,可以有效避免数据被篡改的情况。更重要的是,在计算机网络运行过程中,如果用户身份被他人伪造的话,那么数字签名技术能够帮助用户对数据进行恢复。这两种技术具有安全性高、便于实现以及成本低等诸多优势。另外,通过数字签名技术与身份认证技术可以建立一个安全的通信通道,进而保证通信的安全性与保密性。当用户在进行数据传输时,可以利用数字签名技术来对数据进行加密,并采用数字证书来保证数据的完整性,以此来防止数据被篡改或者丢失等问题。

四、结语

综上所述,计算机网络安全技术作为一门综合性的技术,其应用范围非常广泛,对于计算机网络安全技术的研究和应用是一项长期且艰巨的任务。通过对计算机网络安全技术进行研究,能够有效提升计算机网络的安全性能,提高信息系统的安全性。随着计算机网络技术的不断发展,计算机网络安全技术研究一定会遇到很多问题和困难,这时候就需要上下合力采取有效措施进行解决,唯有如此,才能够保障计算机网络系统的安全性和隐秘性,保护各方权益不受侵犯。

参考文献:

- [1] 赵洁. 计算机网络安全技术的影响因素与防范措施 [J]. 电脑知识与技术, 2022, 18 (6): 40-41, 48.
- [2] 钟震坤, 侯凯文. 计算机网络安全技术的影响因素与防范措施 [J]. 大众标准化, 2022 (14): 146-148.
- [3] 党瑞春. 计算机网络安全技术的影响因素与防范措施 [J]. 网络安全技术与应用, 2023 (5): 171-172.
- [4] 贺云龙, 陆星润. 计算机网络安全技术的影响因素与防范措施 [J]. 科技视界, 2023 (1): 60-64.