2021年12月 普洱学院学报 Dec. 2021
第37卷 第6期 Journal of Puer University Vol. 37 No. 6

计算机网络安全防范技术的研究和应用

田扬畅
安徽公安职业学院,安徽 合肥 230031

摘要:新时代,科技信息技术飞速发展,计算机网络技术已被应用于各个领域,极大地推动了人类社会的发展与进步。但计算机网络安全问题也给用户带来极大困扰,这些安全问题会导致用户的隐私数据泄露,从而带来不可估量的经济损失和负面影响。因此,采取各种行之有效的计算机网络安全防范技术,以此保证计算机网络系统能够可靠、安全的运行。

关键词:计算机;网络安全;防范技术
中图分类号:TP393.08 **文献标识码**: A **文章编号**:2095-7734(2021)06-0031-03

互联网技术的广泛运用,使整个世界都被覆盖在同一个网络之中,人们可以非常便捷地获取所需信息,享受计算机给人类带来的便利。在计算机网络技术广泛运用的背景下,计算机网络安全问题也随之而来,特别是不法分子可以利用技术漏洞来窃取用户信息,以此谋取不法利益。因此,为了保护人们的个人隐私、维护国家安全,就必须要对网络安全使用环境进行积极构建,采取各种行之有效的计算机网络安全防范技术,以此保证计算机网络系统能够可靠、安全的运行。

1 计算机网络安全问题产生的原因

近年来,网络安全问题频繁发生,给人们的数据安全造成了极大威胁,个人重要机密也时常发生泄漏,这对个人、企业乃至国家都造成了极大的损失。为此,只有充分打击网络犯罪,全面杜绝网络安全问题,才能为广大用户群体营造一个良好的网络使用环境,有效保护个人乃至国家的重要信息。对于计算机网络安全问题的产生的原因有多种。首先,设备更新换代快、漏洞多。科技的飞速发展,使得大量新兴技术得以产生,这也使得许多设备及设施变得愈发智能化, 设备设施的功能变得愈发集中, 如果这些设备设施在运行过程中受到攻击,便会导致其无法有效运行,从而给个人、企业乃至国家造成巨大损失。其次,计算机网络环境比较复杂。在计算机网络中,某些组织或个人常常会为了获取不法利益而利用病毒或黑客技术对用户或机构开展网络攻击。最后,价值观取向的差异。在计算机网络技术发展过程中,需要得到全社会的参与,由于计算机网络涵盖了广大的用户群体,而这些用户自身的价值观及世界观有着不同的差异,这也导致其在对计算机网络进行管理与保护时,常常会出现思想分歧,进而使计算机网络的复杂性大幅增加。

2 开展网络安全防范研究的重要意义

对于计算机网络安全来说,需要确保整个网络系统能够在虚拟环境下得以可靠、安全的运行。对计算机网络进行安全保护,需要保证其内部软硬件设备的可靠运行。同时,还要重视系统自身存储数据的完整性与可靠性, 防止数据受到破坏和窃取。特别在大数据背景下, 我国计算机数据正以规模化、海量化的方式快速增长内容。这在某种程度上,极大地提升了计算机网络风险,容易使用户个人的财产和隐私安全受到影响。所以,加强网络安全防范研究是适应大数据技术发展的必然要求。而在经济发展的层面上,信息资源、数据资源在企业经营管理与经济建设中的价值日渐突出,如果企业或组织机构缺乏网络安全防范意识或方法,将导致商业机密、数据及信息受到侵害,严重影响到企业正常运作。因此,网络安全防护是知识经济得以健康发展的有效保障。

作者简介:田扬畅(1962~),男,安徽金寨人,工程师,研究方向:网络安全。
收稿日期:2021-07-23

3 计算机网络安全面临的威胁

3.1 病毒攻击

在计算机网络运行过程中，病毒攻击是计算机网络所需应对的重要安全威胁。计算机病毒的类型多种多样，其目的都是为了窃取用户计算机系统中的重要数据而被制造出来的，还有一些计算机病毒甚至会导致用户计算机发生瘫痪。自计算机出现以来，计算机病毒便随之产生，随着计算机网络技术的不断进步，计算机病毒也不断发展。对于计算机病毒来说，其实质上是一种程序代码。这种程序代码会在用户不知情的情况下被植入用户计算机，并在计算机系统中进行大量复制，同时利用各种途径来感染其他用户的计算机系统，以此对用户计算机系统中存储的重要数据进行窃取和篡改。用户计算机系统一旦被感染，计算机病毒不仅会直接影响到系统的运行速度，使用户的重要数据受到损失，甚至还会导致系统无法正常运行。

3.2 黑客入侵

在计算机网络运行过程中，黑客入侵也是一大安全威胁，用户在使用计算机网络时，网络黑客常常会在未经用户允许的情况下入侵对方的计算机，以此对用户的计算机系统进行数据窃取，或是对信息进行随意篡改，这便会对用户的切身利益造成极大损害。另外，黑客在入侵用户计算机系统时，可以采取多种手段，这些手段往往会使用户难以防范。黑客在实施入侵以后，用户的计算机网络还会产生很大漏洞，而这也会使用户在对计算机网络进行修复时存在极大难度，某些漏洞甚至无法进行修复。可以说，对于计算机网络安全防范工作必须要将黑客入侵作为网络安全问题的防范重点。

3.3 系统漏洞

对于计算机系统来说，其作为人类文明的产物，其自身并不是完美无缺的，在计算机系统运行过程中，常常存在各种系统漏洞，而这些漏洞便是黑客展开攻击的重要途径，同时也是计算机病毒得以入侵用户计算机系统中的通道。一旦黑客在确定攻击目标以后，便会对攻击目标的计算机系统漏洞进行查找，以便开展各种形式的攻击，这势必会导致用户计算机系统中的重要数据被篡改或丢失。所以，在计算机网络安全防范技术研究中，必须要将系统漏洞作为重要的防范重点，确保黑客及计算机病毒不会利用系统漏洞入侵用户计算机系统。

3.4 恶意插件

在计算机网络运行中，充斥着各种软件，这些软件的安全性未知。有些软件中捆绑着各种恶意插件，如果用户下载了这类软件，计算机便会受到网络攻击。这些恶意插件是黑客所植入的，而且恶意插件的隐蔽性较高，一旦用户的计算机系统在安装软件过程中捆绑了恶意插件，黑客便会通过这些恶意插件来对用户的计算机系统进行监听，极大程度的影响到计算机系统的运行速度，甚至会对用户的计算机系统进行攻击和数据篡改。所以，在计算机网络安全防范技术研究中，需要重视这些恶意插件的清除，防止黑客利用恶意插件开展网络攻击。

3.5 硬件运行环境差

对于计算机系统来说，正常运行需要大量硬件的支撑，如果计算机中的硬件运行环境较差，便可能导致计算机硬件发生故障，而计算机硬件出现故障以后，便可能导致计算机系统中存储的重要数据发生丢失。例如在计算机系统中的硬盘便是重要的硬件，当硬盘因灰尘过多或电流过大而发生损坏时，便可能导致硬盘中存储的重要数据发生丢失或损坏，从而给用户带来巨大的损失。

4 计算机网络安全防范技术的研究和应用

4.1 防火墙技术

防火墙是计算机网络安全防范技术中的一种，可以将其看作是一种墙体，以此对计算机系统的内网和外网进行隔离，从而防止外网中的安全风险侵入到系统内网中，保障用户计算机的系统安全。防火墙是由相应的软件设备与硬件设备所组成的，通过在用户计算机系统中设立防火墙，可实现内部网络和外部网络的隔绝，使得专业网络和公用网络得以相互独立出来。在防火墙中包括四大组成部分，分别是验证工具、应用网关、服务访问政策与过滤包，通过防火墙能够对内部网络的所有流入数据与流出数据进行管理。从技术层面来看，可以将防火墙按照两种类型进行划分，分别是双穴网关与标准防火墙。双穴网关是对标准防火墙的一种改造形式，利用双穴网关可以有效隔绝内部网络与外部网络之间的直接联系，如果来自于外部网络的数据包想要进入到内部网络，则需通过双穴网关才能完

成。标准防火墙则是利用相应的管理软件来处理内部网络与外部网络间的通信。同时,该软件还能严格审核用户是否得到授权,不过标准防火墙无法对信息进行第一时间的传递,这使得信息在内部网络和外部网络相互传递过程中会存在一定的延迟性。

4.2 加密技术

在计算机网络运行过程中,需要进行信息传递,这也使信息在传递过程中可能会造成信息发生泄露。因此,为了确保信息的传输安全,就必须在计算机网络系统中充分运用数据加密技术,以此保障信息传输的安全性。在将数据加密技术应用到计算机网络过程中,其具体的技术层次包括三个:分别是链路加密、端至端加密和节点加密。其中,链路加密能够将所有的链路数据按照特定的形式进行加密转换,这样链路信息在网络各个节点中的安全性便得到了极大保障。对于节点加密来说,其节点加密段涵盖了原节点至目的地节点,在这两个节点之间的传输链路能够有效保障其信息安全。而对于端至端加密来说,则是通过特定的加密方式使信息能够从云端用户向着目的端用户进行传输,以此确保数据在传输过程中得到保护。

4.3 漏洞修复技术

在计算机网络安全防范技术中,对于漏洞修复技术来说,需要通过相应的工具对传输数据进行扫描检测,以便于对计算机系统中可能存在的系统漏洞进行查找。当发现计算机系统中存在可能会产生安全风险的漏洞时,便会通过该技术来对系统漏洞进行及时修复,以此防止黑客或不法分子利用该系统漏洞实施网络攻击,这样才能使计算机网络安全得到可靠保证。在漏洞修复过程中,用户可以自行选择通过手动方式进行修复,或是由系统进行自动修复,以此保证网络系统中的漏洞在修复以后不会成为黑客和不法分子的攻击途径。

4.4 网络访问控制技术与防病毒技术

用户在利用计算机网络进行文件传输或是远程登录时,也容易受到黑客的攻击,因此需要通过网络访问控制技术来防止不具备权限的用户入侵对方的网络系统。在网络访问控制中,需要通过路由器来控制外界网络访问。在计算机网络中,路由器可以看作是一种网关,以此对网络中的信息进行过滤,用户也可以通过系统来对文件权限进行设置,并且实时了解自身的访问权限,以确保计算机网络中的信息安全。除了网络访问控制技术以外,防病毒技术能够有效防范计算机病毒对用户计算机系统的攻击。通过对传输文件进行扫描,在发现病毒后,能够将病毒进行隔离和删除,以此防止病毒对用户的计算机系统造成破坏

4.5 云安全

在云计算中,其对海量数据的处理主要是采用并行处理与分布式处理等方法。云安全是以云计算为基础,借助于云计算所具有的强大计算能力,以此对海量数据进行处理的同时,判断海量数据中是否可能存在具有安全风险的危险数据,以此将这些危险数据进行有效剔除。对于于安全来说,其需要通过大量客户端计算机系统来对网络中是否存在异常软件或恶意程序等信息进行检测,然后将检测到的信息利用服务端进行推送。同时,对这些信息作出深入的分析与处理,然后会将病毒清除方案或是木马防御计划发送至各个客服端。通过云安全技术的应用,使得病毒的识别与查杀问题得到了有效解决,能极大程度地提高了用户计算机系统的安全防范能力。

5 结语

总之,随着计算机网络的不断普及,人们在工作生活过程中愈发依赖于计算机网络。同时,计算机网络安全问题无时无刻不在产生着,黑客技术更是随之发展。为了有效遏制计算机网络安全问题,坚决打击网络犯罪,就必须要对计算机网络安全防范技术开展不断研究和创新,使更多的网络安全防范技术成果得以被应用到实践之中,以此有效维护计算机网络中的信息数据安全。

参考文献:

[1] 苏绍培.数据加密技术在计算机网络安全防范中的应用探究[J].信息与电脑(理论版),2020,32(15):207-208.

[2] 赵小冬.计算机网络安全技术的影响因素与防范措施——评《计算机应用基础》[J].林产工业,2020,57(01):115.

[3] 葛小虎.关于计算机网络安全防范中防火墙技术的应用分析[J].网络安全技术与应用,2019,(11):21-23.