试论计算机网络安全问题及其防范措施

◆何泽奇

(重庆工业职业技术学院 重庆 400000)

摘要:在人们的日常生活和工作中,计算机网络成了一个非常重要的工具,随着用户的增多,计算机网络中的安全问题也不断增加。这些安全问题影响了用户的正常使用,而且不利于社会经济的良好发展。为了防止出现计算机病毒以及黑客入侵等安全问题,相关部门一定要加强对计算机网络防护技术的研究,制定出有效的防范措施,为用户提供更加安全的使用环境。

关键词:计算机;网络安全;问题;防范

1 计算机网络安全现状分析

1.1 软件漏洞

软件漏洞的存在是软件的一个不可避免的问题,所有的软件或多或少存在一些漏洞。即使是保障网络安全的防火墙软件,也会存在一定的漏洞,如果不能正确地安装并且使用防火墙软件,也同样会造成网络的安全漏洞。各种其他软件也同样存在软件漏洞,在网络用户使用软件的时候,漏洞问题就会突显出来,安全缺口就会随之打开,不法分子可能会通过软件的安全漏洞窃取网络使用者的各种信息。软件存在的漏洞,导致网络的安全存在很大的隐患,网络使用者的安全得不到保障。

1.2 各种类型的病毒软件应运而生

随着信息技术的不断发展,出现许多病毒软件,许多用户喜欢在计算机中安装各种APP,但是他们不知道的是有些APP是没有经过检验的,这些软件的安全性和稳定性都是未知的。另外,有些用户在不知情的情况下下载了有病毒的软件,这样会导致整个计算机系统的崩溃,病毒软件不仅会危害计算机系统,有些客户的信息和资料也是通过这种方式丢失的,客户的信息安全没有了保障。同时随着现在科技的发达,病毒也在不断的升级、更新,就会产生各种各样的新病毒,因此,要想防范网络的安全,病毒软件的防范、升级、更新是非常重要的。

1.3 人为因素造成的安全问题

人为因素造成网络安全问题,也是造成网络安全问题的一个极大的因素。网络安全问题的解决措施完备的同时需要网络使用者一定要具备安全防范意识。如果网络使用者没有能够正确地使用网络安全措施,那么网络安全问题依旧突出,依旧会危害到网络使用者的使用安全。人为因素导致的网络安全问题,人为的泄露重要的信息,这造成的后果是无法估计的。有许多的网络管理人员,没有足够的网络安全问题解决的经验和足够的信息保密意识,使得网络使用者的网络安全遭受到危害。

1.4 黑客的攻击和侵入

信息时代的发展孕育出许多黑客高手,网络黑客能力极强,黑客的攻击和侵入是当前网络安全中最大的隐患,黑客在无形中对计算机系统攻击,并且不易被发现,一般的网络黑客都是为了获取利益,黑客主要是通过非法手段窃取客户的信息和资料,以达到某种目的,这种形式的攻击和侵入对系统的攻击性非常大,计算机系统内的数据和信息都会丢失和实效,并且随着科技的发展和进步,黑客的能力也越来越强,手段也越来越高超,所以,黑客的侵入和攻击是当下最棘手的问题,也是最难解决的问题。

2 计算机网络安全防范措施

2.1 对网络的软件与硬件加强防护

计算机网络中的软件与硬件是整个系统的重要组成部分,同时也是网络能够有效运行的关键,所以就需要在加强计算机网络安全管理的过程中,重视对软件与硬件的防护,采用合理有效的安全措施对网络系统中软件与硬件涉及到的相关内容、程序与数据进行保护,以确保能够在受到外界或系统中的威胁时,能够拥

有一定的防护能力。在对计算机网络的软件进行防护时,可以重点加强网络软件、数据库以及相关操作系统的安全性;在对计算机的硬件进行防护时,除了要保护与维护计算机的工作环境,也要对其硬件设备以及各种信息储存设备进行有效的保护与维护以及对电子辐射加强防范。

2.2 设置网络防火墙

网络防火墙的应用能够帮助我们有效防范外部用户对企业内部网络的访问或者恶意攻击,还能够对企业内部用户在访问外部可能存在安全隐患网站时进行约束。当企业内的计算机系统实现联网之后,网络安全问题不单是抵抗病毒和系统漏洞预防,另外还必须充分重视对“黑客”的防范,而借助于网络防火墙可以很好地防止源自于外部网络的恶意入侵。将安全软件配置到防火墙之内,借助于这一方式对计算机网络活动予以实时监控,当发现存在非法访问请求或不正常活动时第一时间予以处理,促进网络安全性的提升,还可以借助于网络防火墙来对企业内部网络予以合理划分,让局部的安全问题不会对企业内部网络产生影响。同时,设置网络防火墙可以对网络信息传输与读取进行监控与审核,它可以详细地记录每一次的访问记录并自动生成访问日志,这些日志的生成可以给网络安全维护工作提供十分有价值的信息。如果出现网络安全问题,防火墙能够第一时间进行报警,同时显示问题的具体类型和处理建议。

2.3 采用加密技术

在计算机网络系统的运行中,采用加密数据技术保护网络技术是有效提高我国计算机网络管理水平的重要途径,它是指在网络系统的运行过程中,将节点、链路、端端等多种加密方式相结合,共同做好计算机网络中的数据保护工作。从而确保在传输用户向目标用户传输数据的过程中,更具安全性与可靠性。

2.4 提高用户安全防护意识,培养专业技术人才

网络使用者的网络防护意识薄弱是导致网络安全问题产生的一个重要方面。因此,采取一定的措施,加强网络使用者的网络安全防护意识,加强网络使用者安全意识建设,是非常有必要的。在宣传方面,应当加强网络安全防护的宣传力度,加强网络安全防护信息的传播力度。在教育方面,应当加强对网络使用者法制观念的教育,网络使用者应当全面地了解网络安全的重要性以及信息泄露的危害性,提高网络使用者的法律意识,加强网络使用者的安全防护意识,使不法分子的数量得以减少,利用法律获取不法利益的犯罪率得以降低,降低网络的安全隐患。

在计算机网络不断发展的过程中,人是关键因素,必须培养高水平的专业技术人才,这样可以针对计算机网络的安全问题制定出有效的防范措施。因此,相关部门一定要将培养计算机人才作为重要内容,加大这方面的投入力度,让人们可以系统地学习计算机网络相关的专业知识,让这部分人能够为保护网络安全做出成绩。

结语:综上所述,计算机网络技术不仅要充分发挥自身特点满足人们的应用需求,推进人们的工作与生活,还需要在人们应用的过程中,增加自身的安全性与可靠性。因此,相关的工作人员就要充分认识到计算机网络安全管理的重要性,采用科学有效的手段提高计算机的管理水平,以确保人们在使用的过程中,能够最大程度的减少计算机网络技术为其带来的损失。

参考文献:

- [1]陈丽.计算机网络安全现状与防御技术探讨[J].信息与电脑(理论版),2018(02):154-156.
- [2]孙健,辜雪.关于加强计算机网络安全管理的几点思考[J].科技传播,2018,10(18):124-125.