浅谈计算机网络技术安全与网络防御

吴尚泽　江志晃
广东培正学院　广东省　广州市　510830

摘　要：随着计算机网络的飞速发展，信息化发展已成为人类社会发展的必然趋势，而网络安全问题就成为当前人们最关注的问题。本文就目前计算机网络安全存在的问题出发进行阐述，进而提出一些解决网络安全的对策，仅供各位同行参考。

关键词：计算机网络技术；安全问题；网络防御

计算机网络技术给人们生活带来便利的同时，也带来了极大的信息安全问题，成为当前计算机网络技术发展遇到的重要挑战。目前在各企业的网络中都存储着大量的信息资料，许多方面的工作也越来越依赖网络，一旦网络安全方面出现问题，造成信息的丢失或不能及时流通，或者被篡改、增删、破坏或窃用，都将带来难以弥补的巨大损失。而对于政府等许多单位来讲，加强网络安全建设的意义甚至关系到国家的安全、利益和发展。所以网上信息的安全和保密是一个至关重要的问题。加强网络安全建设，是关系到企业整体形象和利益的大问题。

1 计算机网络技术概述

计算机网络是指以计算机为设备基础并有机结合现代互联网科技的统称。计算机网络是由地理位置不同的多台具有独立功能的计算机及其外部的设备构成， 它们通过通信线路相连，以网络操作系统指挥，在网络通信协议和网络管理软件的协调管理下，使资源和信息得到共享和传递的计算机系统。计算机技术最初的目的就是用于军事计算，使得军事教育的内容和方式发生了根本性的变化，在平时的教学和军事训练中，高度信息化的网络计算机技术不断被应用其中，其广泛普遍的特性使计算机网络技术更好的服务于军事教学和训练，进而提高优化教学手段，加快军事教学的进程和教学的质量。网络时代的到来，信息化、数字化的计算机网络技术已经渗入各个行业，融入我们生活中的每一个角落，其中，计算机网络技术在企业的应用最为广泛带给企业的冲击是最为直接的，它带来的不仅仅不是挑战和冲击，还有机遇，只有牢牢把握这个机遇并充分利用计算机网络技术为自己服务，企业才能得到质的飞跃，成为领军企业的代表。

2 现阶段计算机网络技术存在的安全问题

2.1 网络系统设计缺陷

计算机网络技术要通过其开放性的功能为用户提供用网服务，这样用户才能够利用计算机技术获取到自己所需要的信息，但这种开放式的特征也给用户网络使用带来了一定的安全隐患。在计算机软件开发的过程中，因为开发方式、研究水平等因素的影响，容易造成计算机软件在开发阶段就存在漏洞，使得计算机网络在正常运行的过程中，容易因为这些存在漏洞、缺陷的计算机软件发生严重的故障。事实上，我国在计算机软件开发的过程中，还未建立较为系统完整的市场监督管理体系，从而让一些质量不高、水平较低的计算机软件流入用户群体中，给计算机网络带来极大的安全隐患[1]。

2.2 网络通信隐患

互联网长期处于开放状态下，必然会遭受到一些恶意性的网络攻击，这其中包括地域性技术或者通信协议等技术的恶意攻击。网络通信的核心是网络协议，创建这些协议的主要目的是为了实现网络互联和用户之间的可靠通信。但在实际网络通信中存在三大安全隐患：一是结构上的缺陷。协议创建初期，对网络通信安全保密问题考虑不足，这些协议结构上或多或少地存在信息安全保密的隐患。 二是漏洞。包括无意漏洞和故意留下的“后门”。 前者通常是程序员编程过程中的失误造成的。后者是指协议开发者为了调试方便，在协议中留下的“后门”。协议“后门”是一种非常严重的安全隐患，通过“后门”，可绕开正常的监控防护，直接进入系统。三是配置上的隐患。主要是不当的网络结构和配置造成信息传输故障等。

2.3 网络黑客对计算机网络的攻击

对于计算机网络来说，黑客攻击也会对其产生严重的安全威胁与破坏。所谓的黑客，指的就是在没有得到准许的情况下，一些不法分子通过对特殊技术的运用，登录或者连接他人的计算机以及网络服务器，并且通过对隐藏性木马程序以及指令的运用，获得网络管理权与控制权，最后通过病毒种植的方式，盗取计算机中的一些重要数据，给计算机网络用户带来巨大的损失。由于计算机网络具有自由性以及开放性等特征，所以常常会受到病毒的攻击与破坏。这里所说的病毒主要是指在计

算机程序中安插的病毒，是人编制的对计算机数据以及功能有一定破坏作用的代码。这一代码不但会给计算机的正常使用带来不良的影响与破坏，同时还会导致计算机出现一系列的问题，例如瘫痪问题。计算机病毒主要是通过网络传播的方式，对计算机网络安全产生极大的威胁与破坏，加之病毒自身的传染性、隐蔽性以及破坏力都很强，导致计算机网络的安全很难有效地保证。

3 计算机网络的安全防护措施

3.1 提升计算机网络安全管理意识

由于一部分计算机使用人员自身的网络安全意识十分淡薄，才使得黑客等不法分子有机可乘，最终使得计算机网络安全受到极大威胁。所以，应该将计算机网络安全管理意识全面提高，使得网络道德与心理以及相关法律法规教育等工作得以加强，最终促使广大计算机网络用户能够形成网络安全防范意识，从而更好地应对外来攻击[2]。

3.2 优化系统，弥补系统漏洞。

在计算机网络技术不断发展的今天，我们使用的计算机操作系统肯能不是完美无缺的，由于病毒的不断进化更新，为了防止病毒的侵袭，针对系统缺陷漏洞的补丁程序也应不断的被推出使用。因此，系统开发商应及时更新的系统补丁，计算机用户及时安装使用，避免病毒从漏洞中进入侵害计算机。例如微软公司、诺顿公司等很多软件开发商都开发了相应的系统集成漏洞补丁程序，使计算机用户可以对使用中出现的系统漏洞进行修补。

3.3 加强TCP/UCP端口访问控制

TCP/UCP的端口扫描是指计算机网络向用户主机的各个端口发送 TCP/UDP 的连接请求，并对主机运行的服务类型进行探测。对于恶意程序攻击该部分时， 要先统计外界系统端口的连接请求，一旦发现异常的请求，程序会自动通知网络防火墙实行阻断，对攻击者的IP 和MAC 进行审计。对于一些比较复杂的入侵攻击行为， 例如组合攻击和分布式公职，我们不但需要采取模式匹配的方法， 还要利用网络拓扑结构和状态庄毅等方法来检测入侵，保证计算机的网络环境安全。

3.4 提高计算机网络黑客安全防御

我们电脑中的IP 地址是黑客利用计算机网络技术入侵我们电脑中的重要数据信息的重要通行渠道。因此,保护好我们的IP地址安全很大程度上就可以避免黑客的侵入,尤其是面对LOOP溢出攻击和DOS攻击等。通常情况下个们为了降低黑客的攻击,会采用隐藏IP地址的方式，并加强企业内部的网络安全意识，采用实名制身份验证，降低黑客攻击带来的负面影响。也有一部分的企业，会采用黑客诱骗骗技术，降低非法访问出现的频率，并有效的抵御了黑客攻击，提高了企业网络管理的水平，完善了计算机网络技术的安全防御能力[3]。防火墙是网络安全的屏障, 配置防火墙是实现网络安全最基本、最经济、最有效的安全措施之一。网络接上Internet 之后,系统的安全除了考虑计算机病毒、系统的健壮性之外, 更主要的是防止非法用户的入侵,而目前防止的措施主要是靠防火墙技术完成。防火墙能极大地提高一个内部网络的安全性, 并通过过滤不安全的服务而降低风险。通过以防火墙为中心的安全方案配置,能将所有安全软件配置在防火墙上。其次对网络存取和访问进行监控审计。如果所有的访问都经过防火墙,那么,防火墙就能记录下这些访问并做出日志记录,同时也能提供网络使用情况的统计数据。当发生可疑动作时,防火墙能进行适当的报警, 并提供网络是否受到监测和攻击的详细信息，防止内部信息的外泄。利用防火墙对内部网络的划分,可实现内部网重点网段的隔离,从而降低了局部重点或敏感网络安全问题对全局网络造成的影响[4]。

3.5 重视对计算机网络实行身份认证访问权限设置

网络访问权限主要是指在使用网络时，如果有其他的网络用户想要对计算机进行访问就要通过所设置的准入条件，也就是用准入条件对其他用户进行权限限制，在权限设置时安全可靠是最重要的。因此，在应用计算机时,要对网络访问权限进行科学设置以防黑客、病毒等入侵电脑,减少用户被恶意中害的几率，以此来保护用户的个人信息、文件等。网络访问权限设置的科学性能够为用户的用网安全性提供更好的保障，所以在具体的设置过程中需要相关的网络管理人员对此进行实时的监控,并要对网络权限设置进行优化处理,一旦发现有可疑入侵的病毒，就要马上对网页进行锁定和处理，以此来降低计算机系统被侵害的可能性。

结束语：总之，互联网技术在人们生活中的重要性越来越明显，可谓是家喻户晓，给人们的生活带来了极大的便利。但也正是这些便捷功能的广泛应用使得网络安全问题层出不穷，引起了人们对网络防御的高度重视。因此，在规避计算机网络安全问题时，最先做的就是对计算机技术的安全隐患问题进行分析，然后据此采取针对性的防御措施，最大程度的减少网络安全事故的发生。

参考文献

[1]杨照峰,王蒙蒙,彭统乾.大数据背景下的计算机网络数据库安全问题的相关　探讨[J].电脑编程技巧与维护,2019(12):157.

[2]刘骄剑.用可信计算开启网络安全主动防御时代—— 访中国工程院院士沈昌祥[J].网信军民融合,2019(5):15.

[3]张琰博.数据挖掘在计算机网络病毒防御中的应用研究[J].信息技术与信息化,2018(01):94-96.

[4]唐庆谊.大数据时代背景下人工智能在计算机网络技术中的应用研究[J].数字技术与应用,2019(10):72.