

# 网络安全技术与网络安全运维中的应用分析

李晓雁

烟台市莱山区科技创新促进中心 山东烟台 264003

**摘要:** 网络安全维护对保障计算机中提到安全性有着重要的作用, 计算机网络安全包括隐蔽性、破坏性、突发性等特征。所以相关技术人员在分析计算机网络技术安全时, 必须从多个方面对计算机网络安全进行分析, 确保各项安全软件、防火墙技术及数据加密技术的高速运转, 切实提高计算机网络安全性与稳定性, 提高用户的网络安全体验。本来就当前网络安全技术展开具体的分析, 并提出在网络安全运维背景下的具体应用型策略。

**关键词:** 网络安全技术; 网络安全; 运维运用

## Application analysis of network security technology and network security operation and maintenance

Xiao-yan Li

Yantai City, Laishan District Science and Technology Innovation Promotion Center, Yantai, Shandong Province 264003

**Abstract:** Network security maintenance plays an important role in ensuring the security mentioned in the computer, and the computer network security includes concealment, destructive, sudden and other characteristics. Therefore, the relevant technical personnel in the analysis of computer network technology security, must analyze the computer network security from many aspects, to ensure the high-speed operation of various security software, firewall technology and data encryption technology, effectively improve the security and stability of the computer network, improve the user's network security experience. Originally analyzed the current network security technology, and put forward the specific application strategy under the background of network security operation and maintenance.

**Keywords:** network security technology; network security; operation and maintenance application

### 引言:

计算机技术在为人类带来了诸多便利的同时, 也带来了较大的网络安全隐患。因此, 在安全运维中, 相关工作人员必须根据计算机网络的安全漏洞, 提出针对性的解决方法, 减少安全风险的隐蔽性与破坏性, 确保用户的各项安全隐私得到保护。否则一旦计算机网络安全技术遭受到外部的威胁, 就会对个人以及社会造成巨大的破坏与影响, 降低计算机的公信力度<sup>[1]</sup>。

### 一、计算机网络安全技术概述

计算机网络安全是伴随着计算机网络的发展而带来的一种难以避免的危害, 它主要是采用了相关的管理与技术手段、措施等, 针对计算机在运行过程中的网络数据系统, 进行一定的风险处理, 提高计算机网络安全防范。计算机技术要保护多方面的对象, 对硬件系统、

软件系统要展开相关的数据分析, 避免遭受恶意的攻击或破坏, 防止数据的泄露, 保护个人隐私。因此, 计算机网络安全与用户密切相关, 所以加强计算机网络安全的运维与管理, 对维护用户的相关利益, 保护用户的隐私有着重要的意义。由于社会的发展需要计算机专业的人才, 所以高校必须立足于实际教学, 培养高素质的计算机专业人才, 为他们将来服务社会打下良好的基础。现如今, 许多计算机都存在不同的风险漏洞, 但对于一般的计算机用户来说, 为了确保计算机网络技术的安全性, 就要针对不同的系统软件展开具体的分析, 及时修复计算机在运行过程中的安全漏洞, 避免网络信息被他人非法窃取或篡改。对于计算机网络与运营商来说, 良好的计算机网络系统不仅能提高市场竞争力, 还能赢取用户良好的口碑, 在面对突发灾害时, 确保网络通讯高

效、正常、顺畅<sup>[2]</sup>。

为了弥补计算机在运行过程中的漏洞，高校加强了计算机教育，要求学生必须具有过硬的技术能力，这都是因为高校学生在校进行学习时由于技术不到位、素质能力也欠缺，难以为企业实现全新的创益，自然会被社会所淘汰。因此，高校必须尽快加速课程改革，通过各项行之有效的措施，应用于计算机课程，为信息化发展储备更多的人才。在实际的教学中，一线教师要遵循以学生为本的教学理念，去培养专业的计算机人才，促使当代计算机专业的人才不仅具备较强的专业素质，还能为网络安全发展注入全新的力量。

## 二、计算机网络安全威胁基本特征

计算机网络安全威胁具有三个方面的特征：一是隐蔽性，二是破坏性，三是突发性，相关技术人员要针对计算机网络安全各个基本特征进行分析，采取合理化的措施降低计算机网络安全风险：

### （一）计算机网络安全威胁的隐蔽性

计算机网络安全攻击只需要在短时间内进行操作即可完成，所以具有极强的隐蔽性，所以网络用户在进行具体应用时，稍有不注意可能就会遭受外部的无故侵袭。根据实验数据可知：计算机的网络风险在很多情况下并不是突发性攻击，而是在计算机系统中已经潜伏了较长的时间，只需要在某一个时间点，就会突然得到爆发，造成网络安全问题，所以计算机网络安全威胁的隐蔽性特征，加强了网络安全风险发生的几率<sup>[3]</sup>。

### （二）计算机网络安全威胁的破坏性

计算机网络在进行运营的过程中，对硬盘系统大规模的进行数据重复、读写，可能会导致数据丢失，严重时还可能导致计算机网络系统硬件模块被损坏。而计算机网络风险具有传播快的特点，所以当一台计算机遭受到风险攻击时，由于传播速度的蔓延，很可能造成大规模的计算机网络破坏，对我国社会的整体发展产生较大的危害。

### （三）计算机网络安全威胁的突发性

计算机网络安全威胁没有可参考的规律遵循，并且在短时间内会迅速的扩散与传播。突发性的网络安全会造成大规模的连续性破坏，这是计算机没有建立任何保护机制，会导致正常的运行模式瞬间瘫痪，中断正在运行的各项数据。

## 三、计算机网络安全技术影响因素

计算机网络安全影响因素主要包括三方面的技术漏洞，这三个方面的漏洞都对计算机的安全产生着较大的

影响，降低计算机整体工作的效率，导致计算机安全受到严重的破坏，主要是以下三个方面：

### （一）计算机网络自身漏洞

英特网属于国际网络，这对政府的监管造成了一定的难题，大大降低计算机网络安全的安全性。对于用户而言，有可能只是进行了简单的网页浏览或页面查看等，都会造成安全威胁，导致企业及个人的计算机私密信息遭到窃取。这些风险的产生都是因为计算机网络本身就存在一些安全漏洞，如：常见的Linux系统及MasOS系统和Windows操作系统等，他们的功能设计、主程序、结构配置等方面都存在一定的漏洞，所以会成为黑客攻击的对象，严重降低了计算机网络安全稳定性。此外，计算机网络安全传输、通信协议等方面也存在多方面的漏洞，IP地址的网络时间点不固定，并且不需要身份验证，这种情况下很容易发生假冒，IP地址攻击的状况<sup>[4]</sup>。

### （二）计算机网络自然威胁

计算机网络威胁除了自身漏洞外，还包括大自然的危害影响，主要可能是由极端天气、地震、海啸等外部条件所导致，对计算机的网络线路和设备造成破坏，造成计算机网络安全问题。

### （三）计算机网络黑客攻击

网络黑客作为综合技术要素较高的职业，他们拥有较强的专业性与实践性，善于利用计算机安全技术方面存在的差距，寻找攻击的目标进行恶意攻击，进而窃取用户的相关数据，导致用户的个人隐私受到危害。

## 四、计算机网络安全防护技术分析

### （一）防火墙技术

现如今，计算机网络安全最常用的技术便是防火墙技术，它分为两类，即：过滤防火墙和应用级防火墙，包过滤防火墙是将路由器传送到主机上的数据进行扫描和过滤，进而对数据进行拦截。防火墙既是一种硬件，也是一种软件，更是一种安全过滤部件，它可以将硬件与软件进行融合，对无效信息进行拦截。当相应的数据进行网络输送时，防火墙就能根据访问限制等配件，对数据和信息进行筛选和过滤，进而将外部的侵袭进行隔离，促使传导的信息是有用的<sup>[5]</sup>。

### （二）加密技术

加密技术就是将原本的信息通过数据的加工变为复杂的密文，进而保护数据的安全性，减少泄密发生的几率，加密技术的重点在于加密算法以及密钥管理。加密技术的核心就在于密码保护技术，它包含对称密码、非对称密码以及混合密码，加密技术有多样化的操作，能

促进网络数据中传送的信息在加密技术的应用下更加复杂,保证了传送数据的安全。

### (三) 入侵检测技术

入侵检测技术也就是网络实时监控系統,主要是对计算机的软件系統进行及时的监测,对上传数据库的数据和信息进行对比,当对比后发现可攻击的对象,就要采取措施阻止数据入侵。可采用的方法有:立即将网络进行切断、通过防火墙权限访问进行相应的调整,从而对入侵的数据进行严格的监控,来保证计算机网络安全。另外,计算机网络安全入侵检测主要是包括误用检测和异常检测两种,误用检测安全性高但耗时较长,而异常检测虽然在短时间内能检测出结果,但很容易出现漏洞。

### (四) 网络安全扫描技术

网络安全扫描技术主要是让系统的管理员对计算机网络数据进行及时的监控,随时掌握最新的网络漏洞,并且还可以根据实际发生的状况,采取相应的防范措施,降低网络安全的风险。这项技术的应用对主机、局部网络都要进行相应的扫描,发现问题后即要进行有效的维护。

## 五、计算机网络安全技术在网络安全维护中的有效应用

### (一) 更好地实现数据加密

计算机网络安全需要通过多样化的数据加密来进行保障,数据加密能将基本的数据应用转化为特殊的密码数据,通过不断完善系统的完整性,加强了安全防护,也增加了黑客破坏和攻击用户计算机的成本。同时,黑客在攻击计算机并破解密码的过程中,能够给用户足够的反应时间,将数据进行重新加密或转移,从根本上解决了信息泄露的难题。从目前我国计算机的发展状况来看,加密技术和计算机网络安全之间存在着一定的差别,加密技术可以分为对称加密和非对称加密两种形式,它们所使用的加密密钥是不同的,进一步防止了密钥因为单一性从而被黑客所利用。

### (二) 安装相应的杀毒软件

当前,杀毒软件的应用安装已经成了维护计算机安全的最简便的方式,计算机通过安装杀毒软件,定时对计算机的病毒进行判定和查杀,进而清理系统病毒。杀毒软件的应用可以在短时间内找到病毒,并进行查杀。当下,随着计算机技术的持续优化发展,电脑病毒的形式也种类也在不断发生变化,所以,计算机杀毒软件也实现了进一步的升级和优化,对计算机网络起到了良好

的维护作用。目前最常用的杀毒软件包括:360杀毒、腾讯电脑管家等多项软件,这些软件各有利弊能对计算机的各项数据进行筛选与维护,保证计算机网络安全。

### (三) 合理利用入侵检测技术

利用计算机入侵检测技术,就是将相关的计算机用户的应用程度、网络数据以及系統操作等信息进行收集,以便找寻计算机可能存在入侵的行为,通过警报,刑事拦截入侵行为。入侵检测技术具有主动的安全防护,对信息能进行人为的检测,进而保障计算机安全。当前,入侵检测技术的应用可以分为主机入侵检测、网络入侵检测,它们都有特定的规则为基础,并且对数据进行不断的收集,对数据进行筛选,最后,将检测结果发送到管理员的手中。入侵检测技术起到的作用不同,测试的内容也不相同,需要将多种技术进行结合,才能发挥最大的作用,保护网络安全。

### (四) 加强对计算机专业学生的教导

当前,我国事业单位和企业单位的计算机技术人员的统计大数据来看,这项专业的人才占工作岗位的极大应用比例,而院校着重培养学生的应用性能力得到提高,将教学的重点放在技术培养和理论巩固方面,促使更多的优秀才能服务于社会。由于社会的发展需要计算机专业的人才,所以高校必须立足于实际教学,培养高素质的计算机专业人才,为他们将来服务社会打下良好的基础。高校本应该培养出来的学生既有过硬的技术能力又有文化素质,但在实际生活中高校毕业后却难以找到工作,这都是因为学生在学校进行学习时由于技术不到位、素质能力也欠缺,难以为企业实现全新的创益,自然会被社会所淘汰。因此,高校必须尽快加速课程改革,通过各项行之有效的措施,应用于计算机课程,为信息化发展储备更多的人才。在实际的教学中,一线教师要遵循以学生为本的教学理念,培养学生的计算机学习得到多方面的发展,适应时代浪潮的发展,这样才能为计算机网络安全发展献计献策,为计算机网络安全管理注入新的源泉与活力,促进计算机安全整体的发展<sup>[6]</sup>。

### (五) 建立数据库,防止数据遭到破坏

计算机安全基于数据的加密与保护,相关管理者可以为计算机网络设置加密口令,保护系統网络数据,防止网络被动或主动攻击。这项技术基于密码加密的符号,能促使网络安全得到保护。另外,用户还应该提升计算机的安全使用习惯,增强安全防范意识,加强对计算机网络安全的运营维护,定期对计算机网络进行杀毒与清理,防止潜在病毒的危害。更要建立起良好的资源数据

保护机制,增加计算机网络的安全意识,更换密码口令,防止数据遭受到破坏,造成数据的丢失,对自身的计算机应用造成较大的限制。

#### 六、结语

总而言之,互联网的迅猛发展为计算机带来了许多便利,人们越来越离不开计算机的应用,但也带来了许多不可估量的安全危害。这都是因为计算机网络具有开放性,所以各种各样的病毒也在时时刻刻的威胁着计算机网络的安全性。因此,为了提高计算机网络安全的有效应用,保证计算机系统平稳运行,安全系统的维护对计算机正常运行有着至关重要的作用,相关工作者必须针对计算机网络安全展开具体的研究,保证网络安全的稳定性、高效性以及完整性,为用户提供更高质量的服务。

#### 参考文献:

- [1]常俊杰.计算机网络安全技术在网络安全维护中的应用分析[J].网络安全技术与应用,2020(3):5-6
- [2]熊泽明.计算机网络安全技术在网络安全维护中的应用[J].网络安全技术与应用,2020(3):4-5.
- [3]范海秀.计算机网络安全技术在网络安全维护中的应用[J].计算机产品与流通2020(2):53.
- [4]张玉峰.计算机网络安全技术在网络安全维护中的应用思考[J].数字传媒研究2020.37(1):42-45.
- [5]陈世华,朱佳齐.计算机网络安全隐患与应对措施[J].福建电脑,2009(9)
- [6]石志国.计算机网络安全教程[M]清华大学出版社2008.