

# 探析信息化时代下计算机网络安全问题

汤明星

武昌职业学院

DOI:10.12238/acair.v2i2.7368

**[摘要]** 目前,随着经济环境的改变,网络技术的快速发展,以及网络形态的改变,网络的安全问题越来越引起人们的重视。在信息时代,如何保障计算机网络安全,是当前计算机工作者面临的一个重要问题。基于此,本文通过对当前我国计算机网络安全面临的主要问题进行分析,并针对这些问题进行了相应的对策探寻,以促进计算机网络安全的良好发展。

**[关键词]** 信息化时代; 计算机网络; 安全问题; 策略

**中图分类号:** F224-39 **文献标识码:** A

## Analysis of the Information Age under the computer network security issues

Mingxing Tang

Wuchang Polytechnic College

**[Abstract]** At present, with the change of economic environment, the rapid development of network technology, and the change of network form, the security of network is attracting more and more attention. In the Information Age, how to guarantee the security of computer network is an important problem that computer workers are facing. Based on this, this paper analyzes the main problems of computer network security in our country, and probes into the corresponding countermeasures for these problems, so as to promote the good development of computer network.

**[Key words]** Information Age; computer network; security issues; policy

### 引言

在这个信息化的年代,网络已经越来越渗透到人们的日常生活之中。网络技术为人们的生活、工作提供了强有力的支持。一旦发生计算机网络安全问题,将会对使用者的保密资料及私人财产造成极大的危害。因此,必须要深化对计算机安全问题的认识,并采取有针对性的安全措施,增强计算机网络安全,进而保证计算机正常、高效地工作。

### 1 浅析信息化时代下计算机网络安全问题

#### 1.1 系统漏洞

计算机技术的正常运转依赖于内置系统,而一旦系统出现安全漏洞,就会使计算机中毒。这往往是因计算机网络安全管理模式存在缺陷,在发现问题之后没有立即采取相应的防护措施,导致病毒、木马等软件对计算机的正常运行造成威胁。这种病毒、木马等会收集用户的个人资料,进而使得资料信息被泄露、盗取,给使用者造成了很大的安全隐患。

#### 1.2 信息篡改

目前,各行各业之间的竞争日趋激烈化,有些企业甚至不惜违背法律、伦理准则,利用非法的程序与技术,对敌对公司的计算机系统攻击,以盗取对方的经营方案与资料。如果是这样

的话,对这个行业来说,是一种伤害。同时,部分大学生对网络安全的认识还不够深入,不能很好地保护自己的计算机网络安全。有时候,计算机中的关键资料会遭到不法骇客软件的破坏。另外,由于网络安全机制不健全,也给人们带来了很大的损失<sup>[1]</sup>。

#### 1.3 计算机病毒

计算机病毒已成为当今社会最严重的网络安全问题。当一台计算机被一种病毒感染后,且病毒可在很短的时间里进行复制并对计算机进行入侵,直到计算机死机。当前,电脑病毒有好几种:第一种是木马病毒。特洛伊木马是一种最为普遍的病毒,它经常和软件联系在一起。一般是因为使用者不知道从哪里下载了非法软件,让电脑受了病毒的影响,造成外界的非法监控与侵入,使资讯泄漏。第二种是脚本病毒。脚本病毒在页面上频繁地出现,当使用者浏览与该站点相关的页面时,计算机就有可能被脚本病毒所感染,导致硬盘资料受损。第三种就是“间谍”病毒。间谍病毒的首要手段是对使用者首页进行改变,从而盗取用户的资料。第四种就是蠕虫病毒。这种蠕虫病毒能通过扫描计算机主机,利用计算机软件中的弱点来达到高度隐蔽性,一旦启动,其蔓延速度极快,杀灭起来也更加困难<sup>[2]</sup>。

#### 1.4 操作系统安全问题

当前,大部分计算机用户都在使用 Windows操作系统,而 Windows操作系统自身也有一定的安全性缺陷。计算机对外界因素以及网络安全问题都很敏感。当使用者使用非法软件时,计算机网络安全就会变得更加脆弱<sup>[3]</sup>。

### 1.5 用户主观因素引发的安全问题

当前,很多计算机使用者的安全意识还不够强,这主要体现在:第一,对防病毒软件的安装不够重视,致使计算机易受病毒侵害;第二,防火墙在实际应用中被忽略;第三,对网络上的密码进行简单的设置,不会在很长时间内更换密码;第四,当使用者在公共场合浏览网页时,未将自身的重要资料,如:使用者名称及密码移除。使用者的安全意识不强,会极大地提高计算机网络安全隐患,不利于网络的安全。

## 2 信息化时代下计算机网络安全防护措施

### 2.1 增强操作系统的安全性

没有计算机操作系统,计算机就无法得到真正的应用。当所有的操作都从计算机的操作系统中分离出来之后,他们是不会孤立运作的。计算机操作系统在日常生活及工作中同样易受攻击,这就造成许多安全隐患。因此,在日常应用中,必须对操作系统进行安全防护,以增强系统的稳定运行<sup>[4]</sup>。比如,在一些重要的行业,例如:银行,都要有自己的安全系统。在系统运行过程中,一旦出现安全漏洞,首先由安全系统检测到,然后自动抵御病毒,并针对不同病毒类别的弱点,安全防护系统可进行自我优化,使计算机得到最大程度的保护,进而将损失降到最低。另外,该软件还能对计算机上的防毒应用程序、后端系统的防火墙、计算机中的 VPN等安全应用进行实时监测与管理,当安全缺陷消除后,会自动产生日志,以使有关人员及时发现并防范计算机存在的安全缺陷。

### 2.2 健全有关管理制度

一个可靠的管理系统保证了计算机的实时监测,同时也保证了个人计算机的资料安全。为此,相关管理人员需要在平时的管理工作中,对有关的管理体制进行持续的改进,加大对有关的专业人才的培养,以培养出一批优秀的、专业的、全面的技术人才,进而为产业的发展及网络安全的管理贡献技术力量。另外,也可健全安全管理制度,设立适当的工作组织,对计算机系统的软硬件层次进行定期的测试与改善,以增强软硬件的稳定度,进而保证网络环境的科学性、安全性、有效性。

### 2.3 应用数据加密技术

数据加密技术是一种可以有效地阻止资料被窃取或篡改,以保证计算机网络的稳定运作。因数据可以有多种传送方法,因此用不同的方法传送的数据,也要用不同的方法进行加密。对已加密的数据,使用者只有在解密完毕之后,方可提取资料,而且在解密前,须先核对资料及使用者的使用权限。另外,在对数据进行存储前,必须对数据进行加密,以进一步增强数据安全性<sup>[5]</sup>。

### 2.4 应用漏洞扫描技术

漏洞扫描技术是一种利用全方位扫描手段发现并消除网络

中存在的各类脆弱性的有效方法。基于漏洞扫描技术,可借助扫描软件、安全扫描等辅助手段,实现对计算机系统代码的快速提取与分析,从而能够及时地发现自身存在的缺陷,以制定出有针对性的防护措施。当计算机出现软件弱点时,利用软件侦测技术,可即时提醒使用者修补错误。举例来说,假如使用者的计算机有一个弱点,就可以利用一种自动化的编译与修补软件,在取得使用者的许可及计算机复原之后,就可以修补这个弱点。另外,漏洞扫描能够通过 IP地理信息的认证,采集并整合其中的非法入侵信息,从而有效应对各类网络攻击。

### 2.5 应用防火墙技术

防火墙是一种阻止外来使用者侵入计算机网络入侵的技术,即基于计算机内网与外网的专用网络通讯监测体系,对内网与内网间的信息传递进行有效的控制,从而有效地防范各种危险信息的发生。当检测到的数据不满足使用者预先设定的需求时,防火墙能够迅速地判断出非法的网络攻击,并对违法的信息进行过滤,从而保证网络的安全。一种是应用式防火墙,很大程度上取决于预先设置的代理服务来检测是否存在病毒或入侵,当系统出现异常时,能够及时地对病毒进行拦截,从而实现对计算机的防护;另一种是过滤式防火墙,它通过对多种先进的数据进行过滤,再对路由器进行数据分析。若有安全隐患,则数据资料会直接从计算机外锁住,入不了计算机系统。防火墙的性能是否能够充分发挥,亟需用户对防火墙进行合理的配置。为增强防火墙的效能,防范可能出现的安全隐患,应结合使用者的实际需要及计算机的实际工作状况来设定防火墙。

### 2.6 增强用户的计算机网络安全意识

由于每一项技术都需要使用者正确地设定与执行,因此,使用者必须对计算机网络安全有足够的认识,才能发挥其应有的效能。比如,在使用防火墙技术时,必须要根据具体的计算机环境来进行相应的调整。病毒探测、漏洞扫描等技术都需要使用者按规定的程序运行。因此,用户要主动加强对网络安全的了解,增强自身的防范意识,养成良好的上网习惯,做到不下载、安装、浏览恶意网站。利用杀毒软件,对计算机系统彻底的病毒扫描与检查,从而预防病毒的入侵。另外,在公众场合使用网络时,为防止有关计算机资料的安全性问题,使用后请务必将使用者的帐号、密码等资料删除。

### 2.7 应用病毒查杀技术

病毒查杀技术是一种防护程式,它会在程式中分析出病毒的种类,并迅速辨识出符合病毒查杀特性的病毒,依据病毒的具体类别,自动查杀病毒,并且提醒使用者,以让他们在以后使用计算机的时候能够更好地控制自己的行为。为保证计算机网络安全,在计算机上安装防毒软件,可以达到迅速发现病毒、增强系统运行稳定的目的。虽然市面上有很多免费杀毒软件,但是在扫描和查毒功能上,还是远远不如收费的专业杀毒软件。因此,在有条件的时候,要想取得理想的安全性,就必须购买和安装正规的有偿反病毒软件。

### 2.8 应用入侵监测技术

网络入侵监测技术是一种能够有效地监控和监视网络中的违法行为的技术。按照特定的检测范围,可以将其划分为三种类型:一是误用检测,这种技术可以探测出电脑中已发现的病毒。在对入侵行为进行分析的基础上,对入侵行为进行建模,并对入侵行为进行判定是否为非法侵入。要做到这一点,就必须采取有目的的防范措施,以保证计算机网络的安全。二是异常探测,主要是对系统中出现的异常现象及时进行分析,并采取相应的对策予以排除;三是病毒网络入侵检测。该技术要求在建立数据库的基础上,在数据库中保存病毒及网络攻击的相关信息。利用存取系统,对有关资料进行比对与分析,决定储存于资料库中之数据是否相符,如果两者相吻合,就会被判定为是电脑病毒或者是网络攻击,并采取相应的清除措施。

#### 2.9 出台相应的法律法规

在目前阶段,人们必须加强电脑安全方面的意识。在世界上,信息化水平比较高的国家都把网络安全放在了一个非常重要的战略位置上,并把加强网络安全作为了主要工作。为此,我国相关人员必须从我国网络安全的视角出发,制订专门的法律法规,增强监管能力,并将有关法规付诸实施,号召全社会都要加强对网络安全的基本知识的学习,增强人们对网络安全的意识。当个人或办公使用的计算机遭遇网络安全问题时,以使相关人员可以运用法律手段维护自身的合法权利。

### 3 结论

总之,由于互联网的开放特性,使得用户在使用过程中面临着更大的风险,从而制约着计算机技术的发展。因此,要想从本质上提升计算机网络的安全,发挥其优点,就需要相关技术人员对计算机安全问题进行及时的归纳与分析,以采取切实可行、行之有效的对策,加以解决,从而使计算机技术应用领域进一步拓展,进而为的工作、生活提供方便。

#### [参考文献]

- [1]彭鹏.信息化视域下计算机网络安全问题及防范技术分析[J].无线互联科技,2023,20(08):138-140.
- [2]李好亮.关于信息化时代计算机网络安全问题的探讨[J].数字通信世界,2022,(12):148-150.
- [3]杜宁宁.信息化时代下计算机网络安全防护技术分析[J].数字通信世界,2022,(01):73-75.
- [4]解京璐.信息化时代背景下计算机网络安全防护技术应用与优化分析[J].信息与电脑(理论版),2020,32(13):182-183.
- [5]张旭松.信息化时代下的计算机网络安全防护措施探讨[J].现代工业经济和信息化,2020,10(04):68-69.

#### 作者简介:

汤明星(1984--),男,汉族,湖北孝昌人,大学本科,讲师,研究方向:计算机网络技术。