关于计算机网络信息安全及防护策略分析

于万鹏

（辽源职业技术学院 吉林 辽源 136200）

[摘 要] 随着计算机信息技术的快速发展，对网络技术的应用力度也逐步增大，计算机网络已经在人们生活中占据着重要的地位。当前人们对计算机网络依赖性日益增强，对计算机网络信息安全防护提出了更加严格的要求。面对着计算机网络信息安全威胁的进一步加重，我们应加大研究力度，深入分析计算机网络信息安全方面存在的问题，以便采取合理的解决措施，保证计算机网络信息安全，避免不必要的损失。鉴于此，本文主要分析探讨了计算机网络信息安全及防护策略，以供参阅。

[关键词] 计算机网络；信息安全；防护策略

引言

二十世纪以来，计算机网络技术的发展越来越快，计算机网络技术已经逐渐渗透到了社会的各个领域，而且成为了各个领域中不可分割的一部分。与此同时，计算机网络技术与我们的日常生活的关联也越来越大，计算机网络技术不仅可以让我们的眼界越来越宽，还可以促进社会生产的快速发展。然而计算机网络技术让我们生活品质越来越高的同时，它的危害也逐渐体现，其中最让人重视的就是计算机网络信息安全的问题。这些年来越来越多的计算机网络信息安全的问题已经阻碍了计算机网络技术的进步。所以，为了计算机网络的快速进步，我们必须要寻找新的防护策略来保证计算机网络信息的安全。

1 计算机网络信息安全概述

网络信息安全是指计算机网络系统中的硬件、数据、程序等不会因为无意或恶意的原因而遭到破坏、篡改、泄露，防止非授权的访问或使用，系统可以保持服务的连续性，以及能够可靠运行。对于我国来说，主要是涉及实体安全、运行安全和信息安全三方面。网络安全问题主要涉及五个层次的安全：网络层安全、操作层安全、用户安全、应用程序安全和数据安全。网络层安全就是目标网站识别IP来源，判断其是否合法来源，假如不是授权用户，系统拒绝进入并做记录；系统层安全性主要是病毒和黑客；用户安全性是用户对系统资源访问或使用的权限授权与否，需要身份认证保障用户口令安全；应用程序安全性是用户的和数据两方面；数据安全性是数据的机密性，一般数据保存会加密处理，即使被盗也不会泄密。

2 计算机网络信息安全的重要性

计算机网络安全主要指的是采取有效的措施来对网络系统所包含的软件、硬件设备和其中的数据予以保护，以此来防止由于各类原因而致使其被泄露、破坏以及更改等。其一，因为资源共享是计算机网络所具备的主要特征，其有利于经济、教育以及科研等相关领域工作效率的提升，但这样也会提高其受到各类网络攻击的机率，使得大多数机构在利用网络平台来对相关信息予以发布时，会出现被非法或破坏性访问等相关风险；其二，当前电子与金融等相关系统逐渐渗透到了各个领域中的敏感信息之中，所以对网络信息安全予以有效的维护就显得极其重要；其三，网络信息所具有的安全性，关系到国家经济、政治以及军事等各个方面，并且全球移动通信网也成为各国信息站的主要战略目标，使得网络上的破坏和反破坏、窃取和反窃取斗争变得越发激烈，所以就必须对网络信息存在的安全问题予以全面的防护。

3 计算机网络信息安全防护策略

3.1文件加密和数字签名技术

通过采用文件加密与数字签名技术，能够保证计算机用户信息系统和数据安全保密性得到提升，能够加强对用户秘密数据的保护，避免出现被窃取、侦听及破坏等问题。从加密的实际作用来看，现阶段文件加密与数字签名技术主要包括用户数据利用网络传输、用户数据存储和计算机用户数据完整性开展实时鉴别等方法，对用户数据传输加密技术而言，即加密处理网络传输期间产生的数据流，以此加强计算机用户保密信息通过所有线路的传输安全保护，发送者也可以根据相应加密软件把用户明文信息加密为密文信息。收件人在获得这些密文信息以后，要采用对应密钥进行解密。对数据签名技术的应用，主要是从现阶段网络通信时发生的安全问题对所有电子文档实行的防伪辨认与验证技术方法，以此确保用户数据的完整性与私有性。

3.2安装正规的防火墙及杀毒软件

计算机网络防火墙是提高网络信息安全的重要技术之一，在计算机系统中安装正规的防火墙，能够有效控制网络之间的访问，其主要作用是监控、审计网络信息存取及访问，同时过滤不安全信息。另外还可以对网络资源进行合理的划分，隔离内部重要的网段。防火墙按照应用技术的不同可划分为4种，主要包括监测型、代理型、地址型以及过滤型。防火墙可以详细记录并统计用户网络访问，对存在的可疑行为、不安全行为进行提示或警告。通常防火墙的设置与杀毒软件相互结合使用，杀毒软件具有查杀病毒、抵御木马及黑客程序入侵的功能，需要注意的是要对杀毒软件及时更新升级，提高防御病毒的能力。

3.3及时安装漏洞补丁程序

漏洞主要是因为计算机的程序在进行设定时出现的一些缺陷导致的，这些漏洞是不容易被人察觉的，它们本身对于计算机的危害是很小的，但是会存在一些不法分子对于这漏洞进行利用从而干扰计算机的正常工作，甚至是利用这些漏洞让计算机感染病毒。漏洞的本质是因为计算机程序本身的不合理性导致出现的后台泄露等问题。所以要做好对于漏洞的管理。因为漏洞的出现是不可控的，所以任何软件都可能存在漏洞，但是如今社会越来越多的病毒，都会针对漏洞进行攻击。所以当我们的系统中有漏洞是极大的安全隐患。为了解决这些问题很多厂商都发布了漏洞补丁，就是为了有效解决漏洞。目前主要有360安全卫士和瑞星卡卡等。

3.4入侵检测和网络监控技术

近几年来，入侵检测技术是一种逐步发展的防范技术，其作用是检测监控网络和计算机系统是否被滥用或者入侵的前兆。统计分析法和签名分析法是入侵检测所采用的分析技术。统计分析法，具体指的是在系统正常使用的情况下，以统计学为理论基础，通过对动作模式的判断来甄别某个动作是否处于正常轨道。签名分析法的表现是，监测已掌握的系统弱点进行攻击的行为。

结束语

总之，随着计算机网络在各个领域的广泛应用，其信息安全和人们的生产生活密切相关，必须采取有效策略加强计算机网络信息安全，防止不安全因素对计算机网络系统的威胁，保障计算机网络用户的数据、信息完整及有效，进一步实现我国科技强国的目标。

参考文献

[1]李和平.计算机网络信息安全及防护策略探讨[J].网络安全技术与应用.2017（11）

[2]王家驹，申克.计算机网络信息安全及防护策略浅析[J].数字化用户.2017（02）

[3]于涛.计算机网络信息安全及防护策略初探[J].中国管理信息化.2018（02）