现代计算机技术与应用
2022 年 2 月第 4 卷第 1 期

浅谈现代信息技术安全与防范

张婷婷

重庆工程职业技术学院，重庆

摘　要 | 随着计算机网络技术的迅速发展和计算机网络应用的普及，计算机网络已成为当今社会各领域重要的信息获取、交换和传输手段。虽然网络安全防范技术的研究是目前网络安全研究的一个热点，但目前的技术研究重点仅放在了某一个单独的安全技术上，却很少考虑对各种安全技术如何加以整合，构建一个完整的网络安全防御系统。网络安全问题是当今社会人们甚为关注的热点问题，本文介绍了网络安全的含义和网络威胁的种类，阐述了解决网络安全问题的防御技术。

关键词 | 网络安全；网络安全威胁；主动防御技术

1　网络安全的现状

随着由罗伯特·莫里斯（Robert MorrisJ）编写的一个基于 BSDUnix 的“InternetWorm”蠕虫出现到 2001 年 8 月 5 号的红色代码“CodeRed”蠕虫发作，直至 2003 年 8 月 12 号的冲击波“Blaster”蠕虫的大规模爆发。互联网的安全威胁正逐渐逼近每一个普通用户。进入 21 世纪以来，尽管人们在计算机技术上不

作者简介：张婷婷，重庆工程职业技术学院，大数据与物联网专业。
文章引用：张婷婷. 浅谈现代信息技术安全与防范 [J]. 现代计算机技术与应用，2022，4（1）：11–16.
https://doi.org/10.35534/mcta.0401002c

懈努力，但网络安全形势越发令人不安。在网络侵权方面和各领域的计算机犯罪，数量、性质、手段、规模已经到了令人惊叹的地步。据统计，每年美国由于网络安全问题而遭受经济损失超过了 170 亿美元，英国、德国也都有数十亿美元，法国则有 100 亿法郎，亚太地区的新加坡、日本的问题也非常严重。在国际法律界所列举的现代社会新型犯罪的排行榜上，计算机犯罪已名列榜首。据统计，全世界平均每 20 秒就发生 1 次网络入侵事件，一旦黑客寻找到系统的薄弱环节，用户将会受到相应的损失。根据中国互联网信息中心 2006 年初发布的统计报告数据显示：我国互联网网站有近百万家，上网用户达 1 亿多，宽带上网人数和网民数均居全球第二。同时，各种网络安全漏洞大量存在以及不断地被发现，网络安全风险也无处不在，计算机系统受病毒感染和破坏的情况非常严重，计算机病毒表现出异常活跃的态势。

2　网络安全的含义

网络安全（Network Security）是一门涉及计算机科学、网络技术、通信技术、信息安全技术、密码技术、应用数学、数论、信息论等多种学科的综合性科学。从本质上来讲，网络安全就是网络上的信息安全，是指网络系统中的硬件、软件及其系统中的数据受到保护，不会遭受破坏、更改、泄露，系统可持续正常地运行，网络服务不中断。广义来说，凡是涉及到网络上信息的保密性、真实性、完整性、可用性和可控性的相关理论和技术都是网络安全所研究的领域。

3　网络安全的重要性

在当今的信息社会中，网络信息系统的安全对于整个社会都具有极其重要的作用，大到国家，小到公司，企业，甚至个人，其网络信息系统的安全性都需要得到充分的保护。网络安全体系脆弱将会引发一系列问题：互联网面临大面积瘫痪的危险。引发新一轮利用身份盗窃的网页仿冒和病毒攻击狂潮，从而导致全球互联网瘫痪，从而对通信、金融、交通、广播和众多其他行业带来灾难性影响。

国家利益将蒙受巨大损失。如果电子政务的信息安全得不到保障，电子政

务的便利与效率便无从保证，对国家利益将带来严重威胁。此外，政府网站被攻击、无法访问、网页被篡改等问题的发生都会影响政府的形象。电子商务将遭受严重打击，用户在线购物积极性下降。目前市场调研公司 Gartner 发布的一份研究报告显示，出于安全考虑，四分之一的被调查者表示将减少在线购物，四分之三的购物者表示在网上购物时将更加谨慎。电信运营商形象可能受损，造成电信用户可能流失。计算机系统被入侵是目前电信行业安全状况中比较严重的现象，而计算机系统的受损，将极大地影响运营商的品牌形象，从而导致客户流失。综上我们可以看出在当今的网络时代，信息安全问题已经突出的表现在了网络安全方面，即如何在一个开放的网络环境中保证信息的安全，保证整个信息系统的正常运行。

综上我们可以看出在当今的网络时代，信息安全问题已经突出的表现在了网络安全方面，即如何在一个开放的网络环境中保证信息的安全，保证整个信息系统的正常运行。

4　目前主要面临的网络安全威胁

一般讲，网络面临的安全威胁可分为两种，一是对硬件（设备）的威胁；二是对软件（数据和程序）的威胁。这些威胁的产生可能是自然的、故意的或非故意的，可能来自于外部人员，甚至是内部人员所为。网络的安全威胁主要来自以下几个方面：

（1）实体摧毁

实体摧毁是计算机网络安全面对的“硬杀伤”威胁。主要有电磁攻击、火力打击和兵力破坏 3 种。

（2）无意失误

如操作员安全配置不当造成的安全漏洞，用户口令选择不慎，用户安全意识不强，用户将自己的账号与别人共享或随意转借他人等都会对网络安全带来威胁。

（3）病毒破坏

来自于互联网上的大量病毒通过网络传播计算机病毒，其破坏性高，而且

https://doi.org/10.35534/mcta.0401002c

用户很难以防范。如众所周知的“爱虫”CIH，以及“震荡波”“冲击波”等病毒都具有极大的破坏性。这些病毒以几何级数在互联网上进行自我繁殖，导致大量的计算机系统在短时间内瘫痪，损失惨重。现在，互联网上病毒的种类繁多，不计其数，其对计算机系统的破坏更是令所有的互联网用户以及网络安全专家面临巨大的挑战。

（4）黑客攻击

预先没有经过同意，就使用计算机资源或网络被看作非授权访问。它主要有以下几种形式：假冒身份、攻击、非法用户进入网络系统进行违法操作、合法用户在未授权情况下进行操作等。某些新兴的信息技术在方便使用者的同时，也为“黑客”的入侵系统留下了大大小小的安全漏洞，令系统外部或内部人员可以轻易地对系统进行恶意操作。

（5）网络滥用

在一些企业的内部网上，对不恰当的 WEB 站点进行访问、收发垃圾邮件、利用网络与其他员工或网络用户进行非正当通讯等情况普遍存在，导致大量网络资源的无谓消耗，使网络的使用效率和安全性能大大降低，甚至影响正常的网络通讯。

5　网络安全防范技术分析

面对严峻的网络安全形势，通过以上网络风险分析可以了解网络的薄弱点，从而利用安全技术手段有针对性的去防御。根据近几年网络安全领域的发展情况，网络安全防范技术大致可以分为两类：传统防御和主动防御。

（1）传统防御技术

传统防御技术主要包括防火墙、访问控制、认证技术、病毒防范、漏洞扫描、入侵检测、信息加密技术和灾备恢复等技术。

（2）主动防御技术

主动防御技术是针对传统防御来讲的。传统防御技术为网络信息系统的安全运行提供了有力的保障，但本身固有的缺陷制约了它在网络安全建设中不能更大的发挥作用。其主要缺陷为：防御能力是被动且是静态的，其防御能力主

要依赖于在接入系统之前的系统配置，只能防御系统配置中有涉及的网络安全攻击，而网络安全防护是一个动态变化的过程，新的安全漏洞会不断出现，黑客的攻击手法也不断翻新，传统防御技术是难以识别、检测和处理新产生的网络攻击手段，且只能被动的接受网络的每一次入侵攻击，不能在根本上解决网络安全问题。

6 总结

主动防御技术作为一门新兴的技术，在最近几年内得到了快速的发展。虽然目前防御技术还存在一些尚未解决的难点问题，但这并不能阻碍网络安全防御技术的发展道路。近年来，随着生物免疫技术、神经网络技术和遗传算法等新的概念不断引入到入侵检测技术中来，检测技术也得到很大的发展，目前已经出现了基于生物免疫、基于神经网络、基于协议分析、基于数据挖掘等多种入侵枪测技术研究热点，随着对网络防御技术的深入研究，防御技术必将在网络安全防护中得到更加广泛的应用，成为应对网络威胁、保障网络安全的有力武器。

参考文献

[1] 苏燕电．浅谈构建校园网网络安全，知识与技术 [J]．2007，4（12）：23–25.

[2] 严望佳．黑客分析与防范技术 [M]．清华大学出版，1999：77.

[3] 黄家林，张征帆．主动防御系统及应用研究 [J]．网络安全技术与应用，2007.

[4] B Endicoa．Active Defenseto CyberAttacks．Information Assurance and Security [J]．2006，4（7）：49.

https://doi.org/10.35534/mcta.0401002c

On Modern Information Technology Security and Prevention

Zhang Tingting

Chongqing Polytechnic of Engineering, Chongqing

Abstract: With the rapid development of computer network technology and the popularization of computer network application, computer network has become an important means of information acquisition, exchange and transmission in all fields of today's society. Although the research of network security defense technology is a hot spot of network security research at present, the current technology research only focuses on a single security technology, but seldom considers how to integrate various security technologies to build a complete network security defense system. Network security is a hot issue that people pay great attention to in today's society. This paper introduces the meaning of network security and the types of network threats, and expounds the defense technology to solve the network security problem.

Key words: Network security; Cyber security threats; Active defense technology