

Problems and Solutions in Computer Network Security and Prevention under the New Situation

Song Yue Mei Zhu Zhengqi Zhang

Xinjiang Information Industry Co., Ltd., Urumqi, Xinjiang, 830000, China

Abstract

Under the background of the rapid development of information technology, the emergence of communication network has attracted attention and met the needs of many massive information and diversified communication. Although the application advantages of communication network are obvious, the hidden security risks related to it should be paid attention to, and should be prevented through reasonable measures, and specific measures should be improved according to the new situation. This paper discusses the problems existing in computer network security and prevention under the new situation, and put forward suggestions according to the problems for reference.

Keywords

new situation; computer network; security and prevention; problems; suggestions

新形势下计算机网络安全与防范中存在的问题及解决建议

岳松 朱梅 张郑齐

新疆信息产业有限责任公司, 中国·新疆 乌鲁木齐 830000

摘要

信息技术飞速发展的背景下, 通信网络的出现受到关注, 满足了广大受众多海量信息和多元化通信的需要。尽管通信网络的应用优势明显, 但是与之相关的安全隐患要引起重视, 应该通过合理的措施加以防范, 根据新形势完善具体措施。论文探讨新形势下计算机网络安全与防范中存在的问题, 根据问题提出解决建议, 以供参考。

关键词

新形势; 计算机网络; 安全与防范; 问题; 解决建议

1 引言

近些年, 先进技术的日新月异诞生出众多新鲜产物, 计算机网络在各个领域发挥出强大功能, 成为人们生活、学习和工作中必不可少的组成部分。计算机网络的影响力巨大, 覆盖范围较广, 加之较强的开放性备受关注和认可, 创造了极大的社会效益和经济效益。但是计算机网络特性明显, 在实际应用中也要采取合理的安全防范措施, 这样才能从源头上规避隐患, 避免一系列计算机网络犯罪活动, 强化信息资源安全性和可靠性。

2 计算机网络安全概念

国际标准化组织将计算机安全定义成: “为数据处理系统建立和采取的技术与治理的安全保护方案, 让计算机硬件、软件信息不会因恶意破坏而更改或泄露。”计算机安全重点涵盖着两个方面的内容, 其一是物理安全, 其二是逻辑

安全, 前者可以理解为常说的信息安全, 也就是信息资源的完整性和保密性的保护, 后者则是前者的引申, 重点是指网络信息的可用性保护和完整性保护等。在普通用户的视角展开分析, 主张个人隐私和机密信息在网络传输中受到保护, 不会出现被篡改和被伪造的问题^[1]。从网络提供商的角度分析, 除了考虑这类问题外, 还要结合自然因素、人为因素等采取可靠方案。

3 计算机网络安全与防范的重要性

计算机安全重点体现在信息安全以及物理安全等不同方面, 前者主要是网络安全, 属于网络信息保密性和完整性等获取的支撑条件。当前, 威胁计算机网络安全因素多种多样, 如黑客攻击和计算机病毒等, 应该重视相应的防范措施, 采取合理手段加以干预。在计算机网络运行过程中, 需要关注潜在的安全隐患, 通过合理的落实相关细节, 确保网络威胁防范到位, 进一步完善各项保护措施, 让计算机网络信息更加安全及可靠, 实现保密性和安全性等目标。计算机网络安全问题如图 1 所示。

【作者简介】岳松(1986-), 男, 中国新疆五家渠人, 本科, 助理工程师, 从事网络安全研究。

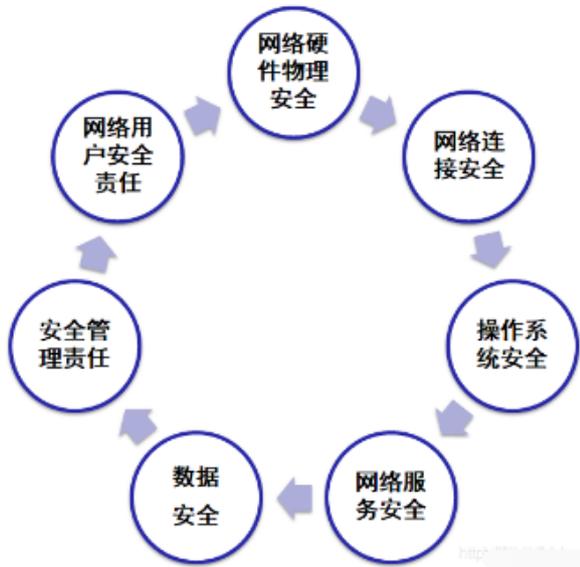


图1 计算机网络安全问题

4 计算机网络安全与防范中存在的问题

4.1 安全问题

4.1.1 病毒侵入

计算机网络在运行环节极易受到病毒攻击，所谓的计算机病毒，就是人为编辑的语言代码，其能对网络造成攻击性破坏，体现出传染性和复杂性等多种特点。在计算机网络中，若是发现病毒问题，必须及时采取应对措施，切断传播途径，降低损失。如蠕虫就是常见的特殊编制代码，其可以在网络环境中不断复制，对于用户的信息安全构成极大威胁，甚至让其使用到的信息严重泄露。此外，在科学技术的飞速发展下，病毒也在更新换代，它们甚至有超越计算机技术的势头，不利于计算机网络的安全。

4.1.2 黑客攻击

近些年，人们的生活水平明显提升，接触到的网络资源日渐增多，面对纷繁的网络世界，极易受到影响，甚至会遭遇黑客攻击^[2]。黑客攻击重点是指在未经法律允许的情况下进入某计算机中，通过对用户数据信息的攻击，使他们的信息资料遭受破坏或者窃取，最终影响到计算机系统的稳定

性，使其处于瘫痪状态。另外，黑客也能将隐藏的病毒程序植入用户计算机中，随着长期的破坏与攻击，使得用户个人信息难以保存，可靠性和安全性逐步降低。对比于病毒，黑客的危害性更强，人为不可控性给黑客的防控带来冲击。

4.1.3 操作系统问题

计算机操作系统是非常重要的组成部分，若是未能及时地完善和优化，将会给病毒和黑客等提供可乘之机，最终影响到安全使用。如果计算机操作系统自身存在着安全隐患，在文件传输环节便会呈现出较多的可执行文件，在防范不到位的情况下，潜在的人为编程文件会在安装程序中出现安装失败的问题，最终影响到软件使用，用户们的信息安全也会受到影响。若是在办公场所，一旦使用了非正版软件，将会出现更多的系统漏洞，可能会引发企业的巨大损失。计算机网络病毒监测如图2所示。

4.1.4 网络钓鱼

在电子商务发展背景下，人们对网购的关注度越来越高，网购带来的便捷性和可选择性备受认可。但是在网购过程中，不法分子也寻找到可趁之机，他们会利用伪造的网站或者是随机向用户发送电子邮件的方式将病毒植入用户计算机，这就使用户交易过程中的信息安全无从保证，用户们的切身利益受到严重影响。

4.2 防范问题

一方面，网络管理人员对网络信息安全的保护意识不强，以至于数据信息出现了严重泄露的情况，多种资源丢失的问题极为常见。计算机管理人员和领导层始终沿用陈旧观念，未能制定出符合新形势的管理制度，使得随意性管理问题突出。系统安全密码没有及时设置，给黑客和病毒的侵入创造了条件，最终引发了巨大的损失，威胁到不同主体的利益。

另一方面，计算机管理不到位，在遇到自然灾害和意外事件时，缺少对计算机信息的科学备份，信息丢失和泄漏情况较为明显，难以发挥出相关信息资源的利用价值^[3]。应该重视未雨绸缪的重要性，要通过科学的路径加以干预，保证及时防范计算机网络安全问题，使得相应的网络环境得以维护，从源头上排除多种安全隐患。

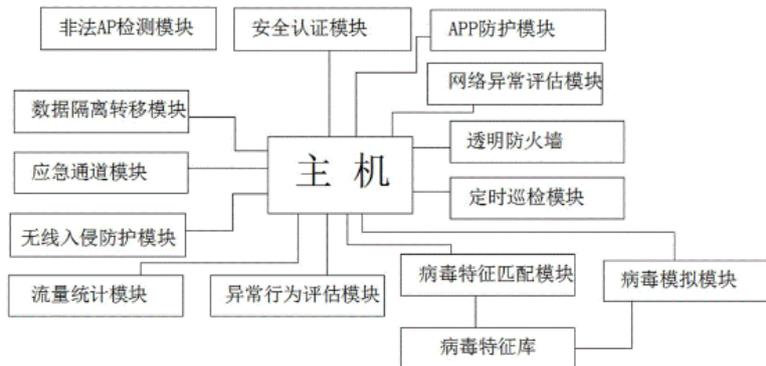


图2 计算机网络病毒监测示意图

5 新形势下计算机网络安全与防范问题的解决建议

5.1 科学选用评估手段，完成病毒查杀

安全状态评估技术重点是对系统落实好整体性分析，在详细的查找环节，明确计算机网络存在的风险隐患，控制其负面影响。在实践过程中，一般是运用恶意代码检测手段，也可通过木马查杀等途径分析情况，如360木马查杀软件就能实现对计算机的定期查杀，进一步强化计算机网络免疫力。为让软件发挥出自身作用，用户应该定期分析软件升级情况，重视软件有效性的提升，以免病毒侵入。此外，在具体的防范环节，还要关注病毒来源，应该尽可能地将多个来源切断，若是涉及访问网站，要及时扫描外来信息，保证无病毒的情况下合理使用，构建起可靠的防范屏障。

5.2 运用防火墙技术，完善权限设置

根据现阶段的情况分析，防火墙技术能够让信息更加安全，同时还能控制网络访问，促使着信息传递过程及时防范病毒和黑客。防火墙技术依照不同网络安全级别，借助于检测信息数据包的方式明确源端口和目标端口等实际情况，确保多种信息可以与访问权限密切联系，从源头上防范病毒和其他隐患，让使用过程安全可靠。防火墙涉及不同的类型，过滤式和地址转换式等均有优势，应该科学的选择，让其进行解包匹配，依照结果向服务器发出请示，实现安全保护的最终目标^[4]。

5.3 优化安全网络系统，强化运行效率

新形势下，计算机网络安全受到的关注度明显提升，为了取得相对显著的成果，应重视安全网络系统的优化，进一步强化运行效率。一方面，局域网重点是将路由器当做边界，将交换机当做传输格局，在具体实践的过程中，设计人员要合理运用分段技术，在科学的控制和管理中，使得具体信息传播更加到位，防范可能出现的潜在隐患与安全问题。通过对应渠道，还能适当地处理非法用户，从最大限度上保障信息可靠性，监督并控制好局域网，让其始终处于稳定运行的状态。另一方面，可以充分挖掘共享式集线器的应用价值，借助于多元化渠道实现上述目标，保证网络运行过程更加稳定，提升基本的质量水平。

5.4 融入先进思路，设置危险陷阱

在实际应用的过程中，除了考虑防火墙与入侵技术外，还要关注陷阱技术应用，其能捕捉危险因素，解决现实问题。危险因素影响较大，将陷阱技术应用到计算机网络中，可以将入侵者引入特定范围，使其在相应的区域进行攻击，保护大范围的安全。根据当前的情况分析，陷阱网络系统重点涉

及蜜罐系统，在具体应用的时候发挥出自身优势，可以模拟不同的操作系统加以诱导，从根本上防范入侵者，保障整个系统的安全。运用相关举措，能够展示出用户的主导地位，还能将多种安全隐患进一步排查，使网络环境更加安全，满足用户对优质服务的需求^[5]。

5.5 提升安全防护意识，拒绝非法网站随意访问

若是实践环节单纯依靠技术，将无法保证网络安全，甚至影响到后续工作的开展。要求用户们积极树立安全防护意识，重视浏览网页中的自主屏蔽意识，若是遇到随意弹出的窗口，应该详细辨别，不可随意点开浏览。如果确认网页不安全，应该及时举报，可有效避免安全隐患。在新形势下运用计算机网络，要重视多种形式，如借助媒体和报纸等加以宣传，提升群众的自我防范意识，以免给黑客和病毒攻击的机会。如果是恶意信息网站，必须及时通过电视或媒体等途径通报，避免用户二次浏览，维护计算机网络环境的安全。

6 结语

综上所述，计算机网络安全防范是一项系统工作，要结合计算机网络特殊性综合判断，还要选择适宜思路优化相关措施，保证信息资源更加安全。应全面了解计算机网络安全因素，对风险隐患着重分析，强化各方主体的安全防范意识。可以从多个角度着手，提升不同主体对计算机网络安全认识，在积极采取多元化防范途径的基础上，将病毒和黑客攻击等及时扼杀，保障计算机网络运行中的安全与可靠。在论文的详细分析中，明确了计算机网络安全和防范问题，在此基础上制定出相关措施，旨在发挥出参考价值。

参考文献

- [1] 宋昭阳,王一诺,王浩文,等.基于Hopfield网络“伪吸引子”与交替量子随机行走的抗攻击彩色图像加密方案[J].电子学报,2014(3):1-13.
- [2] 王丽华.数据加密技术在计算机网络安全实践中的应用——评《计算机网络技术及应用》[J].中国科技论文,2023,18(2):245.
- [3] 龙飞.基于人工智能的互联网络数据安全优化算法研究——评《人工智能在网络安全中的应用》[J].中国安全科学学报,2022,32(11):216.
- [4] 李淼.人工智能在计算机网络技术中的应用探究——以基于人工智能的计算机网络芯片为例[J].中国管理信息化,2022,25(18):194-196.
- [5] 李伟,何明,徐兵,等.基于一维卷积神经网络与改进D-S证据理论的警务云安全数据融合技术[J].计算机应用研究,2022,39(12):3765-3769+3802.