 DOI: https://doi.org/10.26549/bdai.v4i2.13132

The Role and Path Exploration of Computer Network Security System Construction

Zhengqi Zhang Wenbin Guo Li Cao

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

Abstract

The network is one of the most important components in the information age. Under the background of people's demand for computer network, the development of computer network industry is developing faster and faster. While network technology has been popularized to all aspects of People's Daily life, security issues have also begun to enter people's vision. However, in recent years, the frequent emergence of computer network security problems, as well as a variety of hacker attack means, has had a huge impact on the stability of the server. Modern technical means must be adopted to effectively protect the computer network. Based on this, this paper focuses on the construction of computer network security system.

Keywords

computer network; security system; construction

计算机网络安全体系构建的作用及路径探索

张郑齐 郭文斌 曹丽

新疆信息产业有限责任公司，中国·新疆 乌鲁木齐 830000

摘 要

网络是信息时代下最重要的组成部分之一。在人们对于计算机网络使用需求不断扩大的背景下，计算机网络行业的发展速度越来越快。在网络技术已经普及到人们日常生活中的方方面面的同时，安全性问题也开始进入人们的视野。但是，近几年来计算机网络安全问题的频繁出现，以及五花八门的黑客攻击手段，对服务器的运行稳定性产生了巨大的影响。必须采取现代化的技术手段，对计算机网络进行有效保护。基于此，论文重点针对计算机网络安全体系构建的作用及路径进行了详细的分析。

关键词

计算机网络；安全体系；构建

1 引言

信息时代的到来，使得人们的生活方式与工作方式发生了翻天覆地的变化。企业的生产经营效率提高，也能够反过来推动社会经济的改革发展。但是，计算机网络安全问题的存在，不仅增大了各类网络数据与信息文件的丢失风险，还提高了计算机系统大面积崩溃事故的发生概率，甚至使企业遭受巨大的经济损失。必须对计算机网络安全体系的构建予以高度的重视，并探索相应的构建路径。

2 计算机网络安全体系构建的作用

近几年来，个人支付宝账户、微信账户资金莫名丢失问题；部分公司网站因为黑客攻击而无法正常运转问题的存在，不仅让个人遭受了一定的经济损失，还影响了社会经济发展的稳定性。如果一个专门的黑客队伍，对国内军事领域、金融领域以及医学领域的网络基础设施发动定点攻击，那么某一个国家的社会经济发展必然会遭受重创 [1]。要想解决这一问题，就必须不断提高计算机网络的安全性。而在计算机网络当中，要想保证相关数据信息的安全传输，不会出现数据被破坏、信息被盗窃等问题，提升各种软件系统和硬件系统的运行稳定性是基础。所以，必须对计算机网络安全体系的构建予以高度的重视。

3 计算机网络安全问题的出现原因

3.1 恶意入侵

在人为因素的操控下，对计算机网络发动攻击，使计算机网络的稳定运行受到影响，就是一种恶意入侵行为。这种行为的存在，会对计算机网络的安全运行产生严重的影响。分析恶意入侵行为的出现原因，主要与计算机网络安全体系存在漏洞有关。其实，从某种角度分析，任何一种计算机网络安全体系都存在漏洞。如果黑客对计算机网络安全体

【作者简介】张郑齐（1991–），男，中国河南驻马店人，本科，工程师，从事研发及网络安全研究。

系进行研究，并发现了这一漏洞，就会利用这一漏洞侵入网络当中，并对网络中的数据信息进行篡改、盗窃或者破坏，使网络的使用者遭受巨大的损失。目前，人工修补是消除计算机网络安全体系漏洞的主要方式。但是，这种消除漏洞的方式，显然不具有较强的实效性，不能在发现漏洞的第一时间，采取相应的安全防护措施。如果漏洞没有被修补好，就已经被高技术水平的黑客攻击，由此而产生的后果将会非常严重 [2]。例如，某公司的计算机网络使用的安全防护体系，在通信协议方面存在漏洞，由于公司安全专家没有先黑客一步发现这一漏洞，且做好修补工作，致使黑客恶意攻击，对网络中的数据信息进行了恶意窃取和篡改。虽然该公司花费了 7 天的时间修补这一漏洞，消除黑客攻击带来的影响，但是已经产生的损失却无法挽回。

3.2 病毒传播

黑客除了直接利用技术攻击网络之外，还会制造网络病毒。病毒，可能出现在网络环境中的任一“角落”，利用程序捆绑、非法网页等途径，诱骗计算机用户打开通信通道。而一旦通信通道打开，就意味着病毒找到了侵入计算机网络的机会。一旦病毒入侵计算机，就会快速侵占计算机设备的操作权，并对计算机网络安全防护体系的运行产生压制。例如，“熊猫烧香”是 2006 年出现的一种经过变异的网络蠕虫病毒，具有较强的传播能力。在当时，几乎所有的计算机网络安全防护体系，都无法抵抗这一种病毒。

4 计算机网络安全体系构建的路径

4.1 对网络安全管理制度进行优化

为了提高计算机网络信息的安全性，降低数据信息泄露等安全问题的出现几率，需要在计算机管理专业人员、企业以及部分政府领导等人员的共同努力下，对现有的网络安全管理制度进行优化。目前，计算机网络的使用用户已经非常多，涉及社会经济发展的各个领域，既有个体单位，也有企业单位和政府部门。单位属性不同，每天产生的数据信息的价值高低也不同，对于计算机网络使用过程中的信息安全要求也不同。首先，为了加强所有计算机使用用户切身利益的保护力度，必须对计算机网络使用有关的法律监管机制进行优化和完善，并根据用户需求构建一个强大的、完整的、合理的计算机网络安全防护网，对个人、单位以及部门在计算机网络安全中应当承担的责任和需要完成的义务加以明确。其次，在完成网络安全管理制度优化与完善之后，还要对计算机网络安全保护机制进行提高和升级，强化计算机网络的安全防护力度，确保计算机网络用户的隐私安全能够得到保护。只有这样，用户才能够在计算机网络使用方面获得一个相对理想的体验。再次，在构建网络安全管理制度的过程中，需要对计算机网络平台的实际情况进行分析，并以此为基础，采取针对性的防护措施，降低用户在使用计算机网络过程中出现信息泄露问题的概率 [3]。与此同时，还要对用户的使用习惯、使用需求以及使用特征进行分析，并在此基础上提高网络安全管理制度的实用性与科学性。最后，强化网络安全管理制度的执行力度，确保网络安全管理制度的应用优势能够充分发挥出来。

4.2 强化计算机网络软件与硬件的安全性

在黑客技术不断升级，网络病毒不断变异和进化的过程中，计算机网络中的软件系统和硬件系统也应当得到持续的优化和完善，然后借助技术方面的优势，对各种类型的黑客或者病毒进行识别和判断。只有具备较强的病毒识别能力，才能够在病毒传播或黑客入侵时，及时启动防御系统，不让外来病毒找到可乘之机。首先，要对计算机网络中的软件系统和硬件系统进行持续的更新和查杀，保证技术的先进性。软件和硬件是计算机设备的核心构成。软件系统和硬件系统的运行质量、防护水平，对于整个计算机网络的使用安全，有着直接的影响。在使用计算机网络的时候，只有及时更新软件系统和硬件系统，随时检查软件系统和硬件系统，才能够在第一时间发现信息监管的异常问题。其次，针对计算机网络中软件系统与硬件系统的安全性核查，需要做到持续、定期更新，以免软件系统和硬件系统发展速度过快，计算机因为版本老化而面临多种风险因素。最后，还要对软件系统和硬件系统的生产性能质量进行严格的控制，为计算机网络安全性能的提升打好基础。

4.3 加强防火墙技术和防病毒技术的应用

目前，在计算机网络使用过程中，单纯使用防火墙技术，仅能抵挡住未经授权用户的内部网络访问申请，通过内、外网络的隔离，来提高内部网络的安全管理质量，并不能全方位地保证计算机网络使用过程中的安全性。在计算机网络安全防护体系中，防火墙技术的应用最为普遍，主要包含两种技术：一种是包过滤防火墙另一种是代理防火墙 [4]。两种防火墙技术的应用优势对比如表 1 所示。为了将防火墙技术的应用优势充分发挥出来，需要对防火墙技术的漏洞进行有效的识别和修补。另外，防病毒技术在计算机网络中的应用内，可以对网络病毒进行抵抗，保护计算机网络不会遭到病毒的恶意入侵。360 安全卫士、腾讯管家等，都是现阶段应用比较广泛的防病毒技术。在未来的一段时间内，还要继续研发出更多具有更强安全性与防护性的安全软件，借助技术优势，保障计算机信息使用的安全性。

表 1 两种防火墙技术的优势对比

包过滤防火墙	代理防火墙
价格较低	内置专门为提高安全性而编制的 Proxy 应用程序，能透彻理解相关服务的命令，对来往的数据包进行安全化处理
性能开销小，处理速度较快	安全，不允许数据包通过防火墙，避免数据驱动式攻击的发生

4.4 对身份认证和加密技术予以应用

身份认证的双重加密，是现阶段显著提高用户信息安

全的技术方法。在双重身份认证的基础上，对信息加密技术进行充分的应用，可以将信息传输过程中信息被窃、信息泄露等问题的出现几率降到最低。在计算机网络技术不断创新发展的过程中，身份认证与加密技术也应当实现与时俱进，通过人脸识别、视网膜识别以及指纹识别等多种技术保证身份认证结果的有效性，以提升网络信息的安全性。图 1 为身份认证的基本模型。企业单位在对计算机系统进行操作的过程中，会涉及到大量的机密性文件。为了保证这些数据信息的安全性，保障企业的稳定运行与发展，必须对企业内部的计算机系统进行定期的检查和更新，确保能够在第一时间发现计算机系统运行过程中的信息漏洞，并采取针对性的措施进行修补和完善。

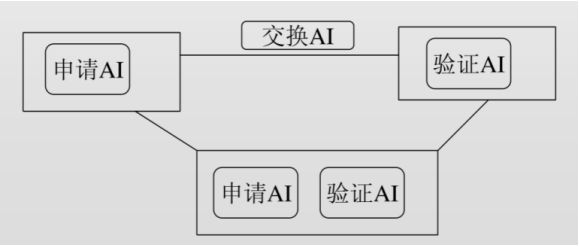

图 1 身份认证的基本模型

4.5 增强用户的安全意识

目前，相当一部分的用户在计算机网络使用过程中，都没有形成较强的安全意识。对此，需要通过各种方式，强化用户的安全意识，确保其在使用计算机网络的过程中，不会因为主观因素而出现信息泄露问题。例如，在设置相关账号密码的时候，尽量不要设置简单的数字或字母 [5]。越是复杂的密码，账号的安全系数就越高。另外，如果某些账号涉及自身的个人隐私信息，还需要进行定期的更换。在使用计算机网络的时候，要养成定期查杀计算机病毒的习惯，针对来路不明的外来链接，不随意点击。

5 结语

随着时代的发展，人们对于计算机网络的使用范围越来越广，使用频率越来越高。要想成功构建计算机网络安全防护体系，不仅要对网络安全管理制度进行优化、对计算机网络软件与硬件的安全性进行强化，还要加强防火墙技术和防病毒技术、身份认证和加密技术的充分应用。另外，还要重点增强用户的安全意识，从主观意识层面，保障计算机网络使用的安全性。

参考文献

[1] 龙广明.大数据时代计算机网络安全体系构建[J].互动软件,2021(12):3246-3247.

[2] 刘开芬.大数据时代计算机网络安全体系构建[J].办公自动化,2022,27(20):16-18.

[3] 毋玉芝.大数据时代背景下的计算机网络安全体系构建[J].魅力中国,2019(19):382-383.

[4] 高博.基于大数据的计算机网络安全体系构建对策[J].现代信息科技,2020,4(12):134-135+139.

[5] 张阳光.大数据时代计算机网络安全体系构建[J].数字化用户,2021(18):57-58.