Education and Learning, 教育与学习(4)2022, 3
ISSN:2705-0408(P); 2705-0416(O)

信息化时代高校计算机网络安全防护技术

肖　军

（汉江师范学院信息化建设与管理处网络中心　湖北十堰　442000）

【摘　要】在信息化时代高速发展的背景下，计算机与互联网已经成为人们生活、工作过程中必不可少的一部分，信息安全作为计算机网络运行过程当中重要的防护措施，能够避免外来的网络攻击，提升网络的运行质量和效率。本文以信息化时代高校计算机网络安全防护技术为主题，分析计算机防护技术概念并解释其重要性，列举信息化时代下计算机网络安全隐患类型，分析信息化时代高校计算机网络安全防护技术内容，总结高校计算机信息安全、网络安全问题并提出相应的优化措施，从而为下一阶段高校的网络安全优化奠定坚实的基础。

【关键词】信息化；计算机网络；防护技术

DOI：10.12361/2705-0416-04-03-76918

由于计算机具备一定的虚拟性和开放性，所以很多不法分子利用网络平台进行非法作业，破坏计算机网络以及网络计算机系统，造成巨大的经济损失，威胁他人的信息安全。所以，如何提高网络安全防护水平是当前网络从业者们所必须重视的一个问题。为提升高校计算机网络安全性，通过使用计算机安全网络防护技术强化系统防护性能，保障网络数据的合法性、完整性以及安全性，提升高校计算机网络运行的稳定性，为后续高校教育工作的开展提供重要助力，确保高校教育系统的正常运行。

1　高校计算机网络安全概念及其重要性分析

计算机信息网络安全能够保障计算机系统在运行过程中抵御来自互联网的恶意攻击，提升系统的运行稳定性，确保系统工作的正常运行。而在高校计算机网络系统当中包含许多重要的信息（学生信息、教师信息、资金信息、个人隐私等），通过构建高校计算机安全网络，能够保证信息在传输、存储过程中的安全性、保密性以及完整性，确保信息在安全系统的监控和管理下不被外来者窃取，保障网络数据的合法性、完整性、保密性以及可利用性。

通过构建高校计算机安全网络，能够提升高校计算机网络的安全性能，避免出现安全制度不完善、操作不合法以及安全事件缺少防御制度等情况，切实保障高校师生的合法利益，为下一阶段高校教育工作的发展以及网络资源的整合和利用起到一定的推进作用。

2　影响高校计算机网络安全的主要因素

网络虽然能够在实际生活、工作过程中为人们提供资源整合和信息传输展示的功能，但同时也会因为信息传输过程中加密措施或保密性不佳，导致信息泄露，从而影响相关事业的发展和经济效益。以高校计算机网络安全为例，目前，影响高校计算网络安全的因素非常多，本文通过对这些因素进行分类讨论，充分说明不同因素的危害情况，希望高校教师能够提升其关注度，避免这些情况出现影响高校计算机网络安全，及时消除相关隐患，保障高校计算机安全防护性能。

2.1　计算机病毒

计算机病毒是早期不法分子利用网络传输的便捷性所开发的一段恶意程序，通常情况下，网络病毒是以程序代码的形式存在且具有一定的隐蔽性，大部分用户很难感知计算机病毒的存在，再加上病毒具有自我复制的功能，一旦计算机病毒满足程序运行条件就可以在短时间之内感染并破坏整个计算机网络系统，致使系统无法正常运行，影响计算机网络的正常工作，轻则造成系统运行卡顿，用户的使用体验降低，重则导致间接网络系统崩溃，出现严重的经济损失。

2.2　来自黑客的攻击

在网络设置当中，有一群利用网络技术进行不正当牟利的人群，这群人被称为网络黑客。他们不仅掌握着丰富的计算机知识和编程技术，同时，也对计算机网络安全有非常深的研究，大部分黑客善于发现网络系统当中存在的漏洞并以此为工具盗取用户的信息进行贩卖，或者使用网络程序对系统运行造成干扰，导致系统陷入崩溃状态，无法正常工作，从而达到牟利的目的。因为黑客本身技术水平较高，难以在短时间之内对其进行跟踪定位，所以在遇到黑客攻击时，很难对其进行有效地遏制，只能交由相应的网络警察部门进行处理。

2.3　系统漏洞

随着计算机网络的发展以及相关技术的更新迭代，很多计算机网络系统在构建之初就留下了系统的漏洞，而这些漏洞是不可避免的。大部分情况下，这些漏洞很难被发现，但是一些专业技术较高的网络从业者可以通过后门以及木马等形式搜寻到相关接口，并利用该接口进行数据、程序以及信息的上传，轻则导致高校计算机网络信息被修改，重则造成学校系统崩溃，难以维持正常的运行。

3　高校计算机网络安全防护技术

虽然计算机病毒、黑客攻击以及系统漏洞的存在导致高校计算机网络安全性能下降，但是在实际生活中，可以通过使用网络安全防护技术，在一定程度上提升高校计算机网络的防护水平，降低外来因素的干扰，以此达到保障系统运行稳定性的目的。本文简要介绍高校计算机网络安全防护技术，希望能够通过这些技术的说明，加强相关高校对计算机网络技术的应用。

3.1　网络安全监测和检测技术

网络安全检测技术是一种被常用于互联网病毒检测、信息检测、系统漏洞检测的技术，其主要功能是找出存在于计算机网络系统当中的各项安全隐患因素并实现精确的定位，为后续病毒查杀、系统优化、网络漏洞封堵提供重要的参考数据。

目前，病毒检测技术在计算机安全领域得到了非常广泛的应用，其工作原理是分析网络侵入行为，并与病毒库当中的侵入代码内容和侵入行为进行比较，一旦发现与数据库当中的行为类似，便将其判断为病毒程序，交由相应的杀毒程序进行查杀。

除此之外，网络安全入侵监控与检测技术还能够监测计算机网络系统的运行状态，并将所有状态记录到日志当中，为后续追查系统破坏病毒来源以及追究犯罪人员相关刑事责任留下相应的证据。

3.2　计算机防火墙技术

计算机防火墙是计算机系统及网络系统当中的重要组成部分，其作用是保障计算机系统安全，防止外来有害信息的入侵，对计算机系统内的有害信息或程序进行查杀作业，从而保障计算机和网络设备的稳定运行。

该技术可以从硬件和软件两个方面进行讨论。硬件方面，可以通过接入网络安全设备，分析传输过程当中的信息片段，以此达到将有害信息阻拦在系统接口之外的目的，避免对系统内部造成破坏。软件方面，可以通过安装杀毒软件对计算机系统进行检查、防护以及查杀，从而实现计算机系统安全性能增强的目的。

3.3　计算机信息加密技术

高校计算机网络系统当中的信息非常重要，具有很高的价值，如果被病毒破坏或者黑客窃取，会造成难以估量的经济损失。而计

算机信息加密技术是基于现实密码学加密所开发的一种加密技术，其原理是通过验证信息端头端尾的字节排列顺序或者端头信息内容，从而达到加密或解密的目的。即使黑客通过漏洞、病毒等方法窃取到相关信息，也会因为信息验证方法的缺失而无法解密该片段信息，从而保障了信息的安全性，提升计算机网络系统的防护性能。

目前，计算机加密技术主要分为 TCP 加密技术和 IP 加密技术，其技术优点分别是加密性能好，但消耗资源大以及消耗资源较少、加密性能较低。可以根据不同的加密内容选择不同的加密方法进行加密，从而实现信息安全快速传输、存储，保障信息的有效性。

4 高校计算机信息网络安全管理问题总结

目前，高校计算机信息网络安全管理问题频发，降低网络系统的防护性能，影响计算机网络系统的正常运行。本文简要总结高校计算机信息系统的问题，希望能够为后续阶段的网络安全管理优化提供重要的参考数据，提升高校计算机信息网络的安全水平。

4.1 学校对计算机网络防护重视程度不足

目前，高校计算机网络系统作为学校运行的重要组成部分，不仅可以帮助学生查询相关课程内容，分析自身综合素质信息，同时也能够找到自己每学期的期末考试成绩，对学生的个人发展以及综合素质的成长有非常重要的作用。但是大部分高校领导层对高校计算机网络信息系统的安全防护不够重视，在高校计算机网络安全系统建设过程中并未将防护技术研究、应用落到实处，再加上现阶段互联网技术发展速度较快，技术更新频率较高，过去的安全防护系统难以对当前的网络病毒、系统漏洞以及黑客攻击进行全面严密的监视、防控，导致部分黑客利用病毒和漏洞窃取学校重要机密文件，造成难以估量的经济损失，威胁高校计算机网络系统运行的安全。

4.2 高素质的计算机安全防护人才

高校计算机网络系统的正常运行，需要由专门的计算机网络安全管理人员进行全天候的监控以及安全问题处理，但是目前从事高校计算机安全网络防护的工作人员整体专业素质较低，掌握的互联网安全管理知识也非常基础，对于计算机网络安全认知不够深入，一旦出现较为突发的安全问题，相关工作人员可能无法做到及时有效的问题处理。

造成这种情况出现的主要原因是现阶段专业素质较高、水平较强的安全管理人才已经被各大民营企业招揽。高校领导层对计算机网络人才的不重视，导致计算机网络安全保护专业人员待遇过低，他们不愿意进入高校体系进行工作，致使我国整体高校计算机安全防护人才储备不足，严重影响高校计算机网络安全系统的正常运行。

4.3 高校计算机网络安全防护宣传工作未到位

在高校运行过程中，学校对人才教育培养的重视程度非常高，所以将大量的时间、精力以及资金都投入到课堂教育当中。虽然新时代多媒体教学设备的引入大大丰富了教学内容，提升了教学的有效性，但是，在信息化发展阶段，高校计算机网络安全防护宣传工作却没有做到位。

大部分情况下，教师针对学生在互联网中可能遇到的各种安全问题没有做出合理的解释以及说明，导致部分学生在浏览网页过程当中点开不明邮件，致使计算机中毒，进而感染整个高校计算机网络系统，威胁高校计算机网络系统的安全。

5 高校计算机网络安全防护优化措施

为提升高校网络安全水平，结合上文对各项安全管理影响问题进行分析，研究高校计算机网络安全防护管理优化措施。希望通过这些方法的有效应用，提升高校计算机网络安全防护性能，保障计算机网络系统的运行稳定性。

5.1 加强间接防护技术的研究，不断更新技术内容

计算机网络安全防护技术是提升计算机网络安全水平的重要方法，同时也是高校信息安全管理体系的重要组成部分。通过加强计算机网络安全防护技术的应用与研究，找出当前计算机网络系统当中存在的问题，并使用对应的安全防护技术进行改进优化，从而提高计算机网络的安全防护性能。

为达到总目标，高校领导层要重视开展网络信息安全培训，加强对计算机网络安全防护技术的认识，重视校园网络安全的宣传和推广。通过分配足够的研究资金给高校计算机网络安全防护系统升级并提供技术性支持，使计算机网络管理人员通过采购硬件或软件的方法提升高校计算机系统的防护性能，避免重要信息被黑客窃取、减少系统漏洞、提高病毒查杀的质量和效率，为后续计算机信息存储传输提供加密措施，整体上加强计算机网络防护力度。

5.2 提升高校计算机网络管理人员技术水平

高校计算机网络安全管理人员的技术水平会直接影响高校计算机网络的安全保护性能。高水平、高素质、专业性较强且工作经验更为丰富的安全管理人员，能够冷静地应对计算机网络出现的各种安全问题并做到及时有效的解决，保障高校计算机系统的稳定运行，降低被其他黑客入侵的可能性。

高校领导层需要从招聘环节入手，对前来应聘的工作人员的工作经验、工作水平、工作资历以及工作思维进行全方位的评析，筛选其中综合素质最优的工作人员进入高校计算机网络工作体系当中进行安全管理工作。并且，在工作过程中提升工作人员的待遇，使其在后续发展过程中能够以积极的心态完成学校交给自己的网络安全管理任务。

5.3 重视计算机网络安全防护宣传工作

在高校计算机网络安全系统管理工作过程中，为保障计算机网络信息安全，所有教师和学生要尽可能地参与到计算机安全防护工作当中，不仅要加强师生对计算机网络安全防护的认知，还要提高他们对网络安全防护的重视程度，确保学生在网络安全教育的引导下，尽可能地积累应对网络安全的经验，掌握网络安全问题处理的方法。

为达到此目标，学校要重视计算机网络安全管理的宣传工作，通过制定网络安全宣传 PPT 以及视频、音频，在校广播站、校电视台和期刊栏进行宣传，提升师生关注度，帮助教师和学生积累网络安全知识，提升网络安全水平，加深广大师生对网络安全防护的认知，从而约束师生使用网络过程当中的行为，减少学生、教师误点不明文件导致计算机网络系统被感染的概率。

6 结语

计算机网络安全对高校教育体系的运行有重要意义，为提升高校计算机网络安全防护水平，本文在明确计算机防护概念的前提下，通过介绍计算机防护影响因素、计算机防护技术、计算机网络管理问题以及网络优化措施，以提升高校计算机网络安全水平，确保高校计算机网络系统稳定运行。

作者简介：肖军（1979.10—），男，湖北丹江口人，中级实验师，研究方向：计算机网络。

【参考文献】

[1] 邱宜宁.信息化时代高校计算机网络安全防护技术探究[J].无线互联科技，2021，18（14）：29-30.
[2] 刘琼.信息化时代高校计算机网络安全防护技术探索[J].信息记录材料，2020，21（4）：109-110.
[3] 孙金超.信息化背景下计算机网络安全技术与防护策略[J].科技经济导刊，2020，723（25）：40-41.