设计研究与应用

数字化校园网络的安全现状及防御对策

韦苏
（吉林女子学校，吉林吉林 132000）

摘　要：科学技术的迅速发展，促使数字化网络的应用日益广泛。当前职业院校加快了数字化校园网络的建设步伐，为现代新型教育教学模式提供了最理想的教学环境，为学生提供了全新的学习工具。在校园网络中，网络安全是至关重要的内容，在数字化校园网络规模日益拓宽的同时，各种各样的网络攻击导致校园网受到巨大的安全威胁。本文根据职业院校数字化校园网络建设的必要性以及安全现状进行分析，并针对现存问题提出防御对策。

关键词：数字化网络；教育教学；安全现状；防御对策
中图分类号：TP393.08　　**文献标识码：**A　　**DOI：**10.3969/j.issn.1003-6970.2022.07.044
本文著录格式：韦苏.数字化校园网络的安全现状及防御对策[J].软件,2022,43(07):155-157+162

Security Status and Defense Countermeasures of Digital Campus Network

WEI Su
(Jilin Girls' School, Jilin Jilin 132000)

【Abstract】：With the rapid development of science and technology, the application of digital network is becoming more and more extensive. At present, vocational colleges have accelerated the pace of construction of digital campus networks, providing the most ideal teaching environment for modern new education and teaching models, and providing students with new learning tools. In the campus network, network security is the most important content. While the scale of the digital campus network is expanding day by day, various network attacks have led to a huge security threat to the campus network. This paper analyzes the necessity and security status of the digital campus network construction in vocational colleges, and proposes defense countermeasures for existing problems.

【Key words】：digital network;education and teaching;security status;defense countermeasures

0 引言

信息技术给生产生活带来的便利性是毋庸置疑的，随着技术的不断提高，校园网络建设也逐步往数字化方向发展。数字化校园网络当前已广泛应用于职业院校，无论是对外交流、教育教学、行政管理、学生管理或是科研开发，数字化校园网络都具有较强的应用性，其对于教育教学和行政管理发挥的作用是无法替代的[1]。但是在深入应用与发展过程中，也逐步显现出更多的安全问题，所以对于职业院校来说，如何最大限度保障数字化校园网络的安全，使其可以为行政管理、教学工作的稳定发挥更有力的作用，成为需要深入研究的问题。

1 数字化校园网络安全建设必要性

保证数字化校园网络安全性，对于维护学校形象具有重要作用。我国现阶段诸多职业院校都已建立校园网络系统，对于日常教学工作、学生管理工作起到了较好的促进作用，如行政管理人员可以在网上办公、传送文件、学生信息管理等；任课教师可以网上教学、共享教学资源等；学生可以网上看书、温习教学内容、回传作业及提出疑问，形成开放、高效的教学模式，促进师生互动，最终实现教育过程的全面信息化。所以一旦系统出现安全性问题，这些数据资料很容易丢失，网络不仅无法稳定运作，学校也会蒙受巨大损失。因此在建设数字化校园网络时，必须要加重视网络安全问题。

2 职业院校数字化校园网络的安全现状

2.1 系统原本的安全性

职业院校数字化操作系统本身具有一定的风险和安全漏洞，因此必须要安装漏洞补丁，促使系统安全性得到提升。但某些学校为缩减数字化校园网络建设成本，

作者简介：韦苏（1982—），女，吉林吉林人，研究生，一级教师，研究方向：计算机应用技术教学。

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

所选用的操作系统与软件都不是正版的。对于盗版软件，微软等运营商都会作出限制，所以一旦出现漏洞必然难以妥善解决，进而导致很多木马与病毒都有机可乘 [2]。

2.2 网络病毒的破坏

网络木马与病毒会给职业院校数字化校园网络带来安全隐患。网络环境中的木马病毒种类越来越多，且种类还会不断增加，在信息浏览、数据传输、资料下载等过程中病毒也会肆意传播，教师、学生的个人资料会被窃取、教学资料丢失无法正常使用等，对用户个人计算机乃至网络整体都会有巨大破坏，轻则会有意外中断的现象，严重的情况下极易使得系统全面瘫痪，资料也会随之丢失，进而损坏系统的硬件。

2.3 硬件设备方面的安全性

网络硬件设备对于校园网的正常运作是非常重要的，其在建设数字化校园网络中也极具意义。具体运行时，校园网络硬件设备会受到诸多因素影响，导致其安全受到威胁，例如人为层面的电源故障、操作失误、电磁干扰、病毒木马等，意外层面的雷击、火灾等。这些因素都极易影响网络硬件设备的正常运行，造成的损坏程度也不同，但都会给网络运作安全造成影响。

2.4 校园网络的安全管理

建立数字化校园网络之后，职业院校还应做好安全管理工作，而管理的范围包括资源配置、站点运作、病毒监测、远程控制等。所以，负责网络安全管理的人员，必须具有较强的专业能力和管理经验，如此才可保障运行过程中迅速解决各类问题。但诸多职业院校在具体管理时，负责校园网管理工作的人员都是兼职教师，如计算机教师等，这些人员在教育教学工作上、行政管理上业务能力很强，但在数字化校园网络安全管理方面，专业技术水平并不达标，网络安全运行知识严重欠缺，要保障校园网的安全运行是存在较大难度的。

3 职业院校数字化校园网络存在的不足

3.1 对数字化校园网络建设未有清晰的了解

通过职业院校各级部门对于数字化网络建设重视度不高，很多人都认为数字化网络建设只是单一的结合校园网与硬件设备，并未由根源上对该建设工作给学校产生的积极影响进行深入认知，导致对此工作重视度普遍较低，这也在一定程度上阻碍了教学工作的发展。

3.2 对数字化校园网络并未做好建设规划

建设数字化校园是推进教育现代化发展的有力方式，目前诸多职业院校都开始规划数字化网络安全建设工作，甚至部分学校已着手建设，但大部分学校开展校园网络建设的出发点都是解决现存的教育教学与日常行政管理工作问题，使得某些工作需求能够得到满足，并未进行深层次的考虑，导致建设规划不够完善，实际的建设效果也不够显著。

3.3 现有的数字化校园网络安全体系不完善

目前有数字化校园网络建设想法的职业院校越来越多，但具体建设方面缺乏完善的运行体系，导致建设工作无法得到有效支撑，加之工作职权并未明晰，管理章程也不够规范与完善，导致在进行数字化网络建设时，职业院校会受到较多的阻碍，所以安全体系的建设一直处于较为滞后的状态。

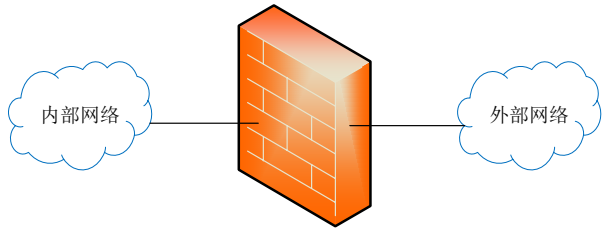
4 职业院校数字化校园网络安全防控体系及切入点

4.1 物理实体安全防控

建设服务器机房时，必须要依据国家的标准进行，且要严格管理配电室、计算机机房等重要的部门，并做好系统的定期维护工作，同时记录好维护日志。必须要针对突发事件制定应急预案，确保有任何事故出现都可第一时间处理，而一些重要的设备还要让专人负责管理，这样才可使得设备始终处于稳定的运行状态，避免事故出现后给整体的系统造成更大的危害 [3]。

4.2 网络安全隔离防控

网络架构包含了诸多内容，而首要的设备为路由器。黑客往往会将路由器作为首要的攻击目标。因此，要设置过滤规则，将屏蔽的 IP 地址过滤掉。防火墙负责系统各端口的监控工作，其借助和网络相连的数据包，对于所有的访客都会核实身份，外部用户也会限制其进到内部网中，且一些不安全的服务也会过滤掉，非法用户没有进入的机会，如图 1 所示。IDS 安装的部位为计算机网络的核心部位，主要对网络上全部的数据包进行监测，用于对网络与信息系统异常的访问行为进行实时监测，目的在于对恶意的动作进行捕捉，并快速发出警告。其和防火墙的差异性主要体现于，依据指定规则来实时扫描与监测端口，可以第一时间发现入侵者，并以较强的识别能力，对于防火墙难以识别的攻击进行制止。网闸主要是用于物理隔离和信息交换，其属于安全隔离系统，其应用的



防火墙

图 1 防火墙

Fig.1 Firewall

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

也是物理隔离技术。包含防火墙、路由器等内容，都是用于异常行为的监测以及对外部入侵进行阻止的，此方面都是网络安全隔离能够切实实现的重要策略。

4.3 网络主机安全防控

（1）操作系统必须要保障安全性，系统若是盗版的，那必然会影响操作，且在保障系统为正版的情况下，还应实时进行更新。同时，还应保障操作系统当中没有不必要的系统组件，那些多余的组件都应删除。操作系统也应对服务进行合理裁剪，将那些不必要的服务与端口全部关闭，并把非必要的磁盘文件清除。（2）数据库必须要保障安全性，做好备份与恢复工作，可使得数据更为完整与安全，可以只对数据库进行备份，也可以对数据库及增量数据进行备份，备份工作是尤为重要的，其是最为直接的解决数据安全问题的措施之一。（3）密码技术必须要保障安全性，在信息安全方面密码技术为核心技术，其在信息安全方面起到了极大的保障。频繁的监测与扫描服务器当中的文件，通过防病毒卡对文件访问的权限设置。同时，对数字签名和认证系统应不断完善，确保经过身份认证后才可查看相关文件与数据，且文件与数据都应保障完整性，留下证据避免源发送者不承认的情况出现。（4）虚拟机必然要保障安全性。虚拟机这个系统是可以让多个操作系统共同运行的，可使得底层硬件得到更有效的使用，在同一个电脑中虚拟机可以共同使用几个 OS，且所有的 OS 都可进行隔离，操作起来也非常便捷。

5 职业院校数字化校园网络安全的防御对策

5.1 防水墙技术

防水墙技术也是网络安全技术的一种，其是基于防火墙技术之上发展的，它的作用和防火墙恰好相对应，是避免内部信息会朝外扩散。防水墙可借助密码限制、访问控制等手段，来保护重要的数据资料，避免黑客入侵，也更好的保护系统资料。职业院校在利用防水墙的技术后，对校园敏感信息可进行更好的阻止泄露，网络安全在事前、事中、事后整个过程都能够得到较好的保护。该技术和防病毒产品并不冲突，反而是和这些产品进行配合后，能达到更好的保护效果，网络安全系统也将更为完善。

5.2 病毒防范技术

计算机网络病毒当前的种类不断增加，且在持续演变过程中愈发复杂，且也有更强的隐藏能力，杀毒软件对于这些病毒也无法及时发现与清除，导致在很大程度上影响了计算机的安全性。所以，及时查杀和防范病毒，是计算机网络安全得到更好保障的基础之一。我国目前的很多职业院校，对于校园网安全管理，几乎都是采用安全防火墙、更新病毒数据库、购买杀毒软件、定期安全扫描等病毒防范措施。除此之外，还要限制非法网站，非法下载链接，自动屏蔽一些可下载的非正常资源，也可对病毒起到有效的防范。

5.3 入侵防护技术

入侵防范技术属于网络安全技术的一种，其有显著的主动性，对于非法入侵行为可实时发现并快速阻止，使得网络安全得到更好的保护。职业院校目前采用较多的是 HS、AIP 等入侵防护技术，只要有网络系统漏洞出现，并有攻击行为，该技术将会积极寻找这些攻击行为并快速阻碍，这对于校园网络安全可起到极佳的保护效用。

5.4 信息数据加密技术

信息数据加密技术也是主要的阻止黑客攻击的手段，其在职业院校中也已取得广泛应用，尤其是数字化校园网络建设方面。该技术传输储存有两种加密类型，一种是传输加密，包含有端到端、节点、链路三种加密方式。以端到端为例，端到端加密确保只有通信双方，即信息的发送方和接收方可以对数据进行处理，如图 2 所示。在网络传播过程中，其可结合 OSI 的层次为数据自动选择适宜的加密方式，也就是数据传输全过程都会做好加密工作，避免传输时有被破坏的现象。另一种是储存加密，是对硬盘中存储的数据进行加密，如此一来黑客即使盗走了数据资料，但如果解密信息不正确，真实的信息也难以被黑客盗走使用。

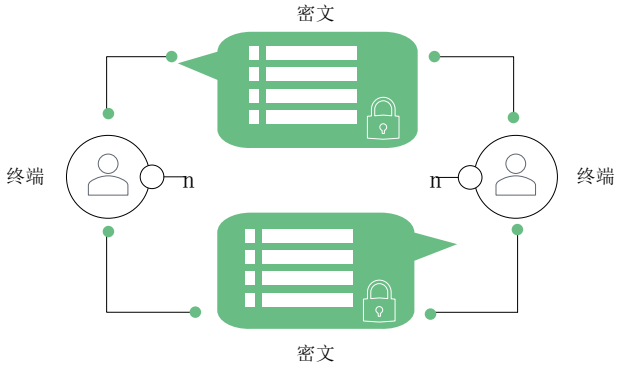


图 2 端到端数据加密技术

Fig.2 End-to-end data encryption

6 完善职业院校数字化校园网络安全建设的方法

6.1 提升师生对数字化校园网络安全的认识

职业院校的教育教学工作中，主体已不单单是师生，负责建设数字化校园网络的人员也是非常重要的组成内容，校园网能否取得良好发展，和此类工作人员也有着密切关系。所有负责建设工作的人员，都要强化对

…… 下转第162页

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

参考文献

[1] 赵志峰,赵曦滨,陈丹宁.多维MANET可靠性建模研究[J].计算机科学,2018,38(5):60-64.

[2] 何明,肖登海,裘杭萍,等.一种移动Ad hoc网的可靠性评估方法[J].计算机应用研究,2019,26(11):4282-4285.

[3] 乔晓东,毛志,邓宏钟.网络端端可靠度的上下界计算研究[J].电子设计工程,2018,19(17):94-97.

[4] 闵军,张海呈,朱桂斌.自组网可靠性评价方法[J].电子科技大学学报,2018,37(3):436-438.

[5] 戴沁芸.无线自组织网络容量研究[D].武汉:华中科技大学,2016.

[6] 王栋平.物联网传输及网络可靠性研究[J].科技创新导报,2020,17(15):163-164.

[7] 李维,冯钢,刘冬,等.物联网系统安全与可靠性测评技术研究[J].计算机技术与发展,2019,23(4):139-143.

[8] 李维,苗勇,汤业伟,等.物联网系统可靠性检测与评估技术[J].软件,2012,33(4):1-4.

[9] SHEN D G,Horace H D Ip.Discriminative Wavelet Shape Descriptors for Recognition[J].Pattern Recognition,2018(32):151-165.

•••••• 上接第157页

校园网络建设的认知，并积极向师生宣传这项工作的意义，促使师生在教育教学过程中积极应用数字化手段开展教学活动，实现数字化网络的最大限度利用。

6.2 数字化校园网络安全建设应进行科学规划

校园数字化网络建设若要确保其能够实现更好的发展，必须要进行科学规划，因而职业院校在此工作规划方面必须要高度重视，对全校师生进行校园数字化网络使用培训，使全校师生学会使用数字化网络的同时，还要注意网络安全，保护好校园网。同时，应开展系统化的培训工作，对计算机教师和各科室专职人员进行更深入的长期系统学习，避免和解决在使用校园网过程中对网络安全和硬件产生的不良影响，除了校内的专业人员需要加大研究力度，也可积极引入校外的专家进行辅助，由此更好的保障工作的科学性，使得最终的建设与应用效率可达到更高。

6.3 数字化校园网络安全管理体系的完善

在此建设工作开展过程中，学校必须遵循当地教育部门下发的要求，遵循上级的安排，确保各部门的效用都可最大限度发挥出来，同时要建立相应的管理与评价机制，为体系的安全运作提供有力保障。而对于体系现存的不足，必须要寻找到原因并有针对性地进行优化与完善。

6.4 加强校企间的合作

职业院校和企业的合作形式也应朝着多样化方向发展，双方之间加强合作，不仅可为安全建设奠定良好的资金保障，且企业也能够通过和学校合作来优化自身的技术团队，弥补人才的不足，也可不断提升技术。应重点关注的内容是，职业院校在合作企业选择过程中，要选择有较强技术实力且在自身发展领域中有一定成绩的企业，且对企业累积的经验和实践水平也应有充分了解，并在后续的企业系统开发时让学校人员参与其中。总的来说，学校自身的知识与技能储备也必须有较高的要求，这样才可建立更优质的技术队伍，并在校园网建设时可充分发挥效用，确保校园网的安全运行。

7 结论

数字化校园网络为提高教育教学信息化水平和工作效率提供了一条科学的、可行的和必行的途径。而我国的职业院校在数字化校园网络安全建设方面，尚处于起步阶段，缺乏较好的基础，且发展速度并不快，又不能直接套用本科院校的做法，因而必须要彻底转变观念，对此工作引起高度重视，对师生进行使用培训学习，加大技术方面的投入，和企业进行积极合作，切实将建设与维管工作落实到位。

参考文献

[1] 张宗法,侯峰.数字化校园网络的安全现状及防御对策[J].网络安全技术与应用,2021(12):86-88.

[2] 苏治中.数字化校园网络安全防范机制构建及实践分析[J].电脑知识与技术,2021,17(16):40-42.

[3] 陈晓凤.数字化校园建设工作中计算机技术的具体应用[J].电脑编程技巧与维护,2020,(12):159-161.

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net