高校信息化建设进程中信息安全问题及对策分析

徐绍铜
广州工商学院　广东　广州　510850

摘　要：高校信息化“以高性能校园网为基础，实现学校管理业务流程的合理重组和管理职能的转变，形成高效的、充满活力的新型管理机制;实现教务管理、教学资源管理、科研管理、后勤与服务管理的全面整合，进-步提高学校的综合竞争实力”。计算机网络技术的应用变革了高校的教育模式、教学方法，增强了高等教育的开放性，促进了教育的现代化发展。然而由于计算机网络具有开放性和互联性的特点，每年国内外政府机关、企事业单位的网络都不断遭受到黑客、恶意软件、病毒、后门程序的攻击，严重影响了国家的安全、社会的稳定和人们的生活。因此，研究信息的安全问题有着重要意义。

关键词：高等学校；信息化建设；信息安全问题；对策

1 高校信息化建设中信息安全的重要性

近几年我国互联网技术在不断的进步，计算机网络的应用已经存在于各个高校之中，同时逐渐涉及到不同方面，各种技术的运行都有关于计算机的信息存储以及信息传输等方面，而有关信息安全的问题是这其中最为关键的一点。大多数教学中，教师会使用到一些软件进行辅助教学，因此这就需要人们将关注的重点放到信息网络的安全问题上。若使用的设备或者网络的安全情况存在危险，则教学上的一些关键信息以及教学资源很有可能会被窃取或者丢失，如此情形一旦产生将会给高校的正常运作带来极大的不利影响。因此，在高校的信息化建设进程中，信息安全问题至关重要的一部分[1]。若想保障学校信息不被窃取或丢失，就应该清楚的了解信息建设过程中出现的问题，及时提出良好的应对方案。

2 高校信息化建设中存在的安全隐患

2.1 信息技术自身的安全隐患

信息技术以计算机为核心，计算机中的病毒则是危害信息安全的重要隐患之一。计算机病毒通过对计算机中的数据造成破坏，影响计算机正常运营，甚至对计算机系统功能造成毁灭性打击。随着信息技术应用于人们日常生存生活的方方面面，各类信息都已数据形式储存，一旦计算机病毒对数据造成侵害，将严重打乱人们有序的生产生活。与此同时，信息技术的迅猛发展，使得纷繁复杂的各类型APP竞相进入人们的视野，大量的软件下载使恶意和非法软件有了可乘之机。这些病毒软件通过非法窃取用户个人信息对用户隐私造成巨大威胁，甚至严重影响用户生命财产安全。不仅如此，电子邮箱威胁也已经成为不法分子实施犯罪行为的途径之一。通过将大量垃圾邮件发送给校方，造成邮箱拥堵，使得校方无法正常发送校园邮件，教务活动也相应受到影响[2]。

2.2 人才缺乏，技术相对落后

“任何安全设施和安全产品都需要专业管理人员的审核、跟踪和维护”，因此，高校信息系统管理人才的素质在很大程度上直接影响着高校信息系统的安全。目前，我国很多高校的网站容易遭到攻击的一个重要原因就是管理人员没能及时更新系统补丁程序。“虽然我国信息技术发展迅速，短时间内已经取得了很大的进步。但与发达国家相比，我国的计算机技术和软件技术仍然比较落后，导致我国的软件安全技术落后，赶不上病毒、黑客发展的技术，在技术上无法确保企业信息系统的安全”。同时，资源没有得到有效配置，如有些高校只是在硬件与软件进行投入，对于专业化的信息安全技术人员很少引进、培养和提高，有的规模较小的学校往往只有一两个技术人员，这使得高校“要么是信息安全人才极度匮乏，要么就是信息安全人员专业素质不高，很难肩负起信息安全责任，从而导致高校信息安全防护措施处于较低水平，当出现新的攻击事件时无能为力[3]。

2.3 高效内部信息安全管理意识、水平不到位

正所谓意识决定行动，虽然越来越多的高效加入信息化建设队伍当中，但是在信息安全管理方面还没有形成足够的危机意识，也没有形成完善的应对方案。部分高校虽然表面上开始筹建信息化建设，但是实际管理工作仍然沿用传统方式，如此形式大于内容的表面文章知识阻碍高校信息化建设的步伐，降低管理水平。不仅如

基金项目：本文系广州工商学院高等教育教学改革项目“基于腾讯微校生态圈的质量工程项目监控研究”

此，由于高校学生流动性强以及校园网络非限制性应用的客观事实，如果忽视信息安全管理，那么如此强的人员流行问题，以及网络非限制问题都将对高校信息安全造成威胁，校内各项信息数据都将面临损坏和泄露风险。

2.4 高校内部关于信息安全的管理水平低

虽然大部分的高校都已经进行了高校信息化建设，但是在信息安全管理方面的意识和管理水平还存在严重的不足。部分高校在建设了高校信息化之后仍然采用传统的学校管理方式,与信息化建设管理非常不利。高校必须加强对信息安全问题的重视和对信息化建设的安全管理[4]。若不加强信息管理,高校大学生极强的人员流动性、学校网络的应用非限制性都将使高校的信息管理系统、学校各项信息数据面临毁坏和泄露的威胁。

3 高校信息化建设中解决信息安全问题的措施

3.1 建立完善的信息安全管理系统

俗话说“无规矩不成方圆”没有科学完善的安全管理系统作为支撑，很难保证物流管理工作可以高效、合理地进行。因此为了切实解决高校信息化建设进程中安全管理系统建立方面应从以下方面着手：

3.1.1 校方务必建立明确的管理制度，对于网络技术相关问题进行明确的制度规定。例如明令禁止师生下载非法软件。

3.1.2 为了降低因为意外事故导致的数据流失问题发生，应当由相关负责人对网络信息中的重要数据要及时做好备份。

3.1.3 加强对管理人员进行专业化培训，提升人员素质水平。再先进的网络技术手段终究离不开人的操作。因而为了有效避免校园信息系统被入侵，或者即使被侵害也有足够的专业知识以及技术手段加以解决[1]。为了培养出更多专业型人才，高校势必要加强对信息安全管理专业人才的培养战略，加强职业培训并形成长效机制，通过建立健全一整套完善的公开透明的高校信息化建设人员管理办法，将绩效考核体系和工作培训机制以及奖惩标准等加以说明，从根本上提升员工的工作热情也有助于提升员工的工作能力和操作水平，打造高素质高校信息化建设管理工作队伍，让高校信息化建设管理工作者向着科学性、条理性方向迈进，这样才能满足时代发展的新要。

3.1.4 校方要加大对高校信息化建设信息安全管理的资金投入，通过充足的经费支持作为前有力的后盾，确保校园信息化进程排除万难、稳步向前。

3.2 加强信息化建设管理

首先要提升校园网络安全意识，对校园中使用网络的相关人员要定期进行安全教育和培训，强化每个人的信息安全意识，并将维护信息安全责任落实到每个人的身上，毕竟个别人的力量太薄弱，难以形成坚不可摧的保护屏障，只有每个人都从内心深处形成对网络信息安全的高度重视，在使用网络过程中自觉形成接受保护的意识，只要这样才能为高校信息安全构筑坚实的屏障，将因软件失效导致信息系统被病毒侵入现象变成小概率事件甚至转变为不可能发生事件，从而提升高校信息化建设效率[2]。

3.3 加强工作人员培训与安全教育，提高安全意识，落实安全职责

在高校信息化建设过程中，学校应该认识到，高校信息资产对于学校信息化建设和发展有着更为重要的地位，高校信息安全防护间接地影响着高校管理水平和管理能力，影响着高校的核心竞争力，在某些特殊条件下，甚至会影响高校的生存和发展。因此，必须站在高校发展的战略高度来看待信息安全，充分认识到其在高校信息化建设中的重要性，加大信息安全投入，提高信息安全人员素质，围绕高校信息化建设的总目标和总体策略，科学采购和建设硬件，加强信息安全技术人员的专业素质，积极开展各种信息安全宣传教育活动，定期对员工进行信息安全教育培训，结合科学的信息安全管理理念，使高校信息安全防护实现最优化。

3.4 制定安全计划

I知识为基础的机构如图书馆、人力资源或I部门的参与，将加强ISA倡议的目标，而不需要详细的职责和计划，以实现ISP的发展目标。然而，ISP不能保证做出正确的决定，但它提供了关于目标、指标和进展措施的综合观点[3]。利用ISP的主要重点是视觉翻译，将愿景与过程联系起来，制定确定优先顺序和资源重点的计划，因此，需要反馈和学习经验的评价来衡量未来功能的绩效，如修改计划和制定可信的措施。

3.5 提高安全意识

高校保护信息的政策往往不起作用，原因是学生和教职员工对信息的重要性认识不足，对当前案件的预期反应不足，信息安全的优先级较低。以ABC模型为基线的三个不同的人的因素产生了三个相互关联的成分，它们强调知道、感觉和行为之间的关系，从而决定ISP的成功。本文从人类因素扫描的三个方面进行综合研究，衡量环境意识的程度，找出进一步可行的改进步骤，以及与其他政策相一致的过程，以保持竞争优势。大学对重要或关键信息的利用，会对作为社会学习和实践场所的大学的公信力产生负面影响。ISA具有识别、衡量和

激励影响、贡献和效应的重要作用，应成为ISP发展的第一要务。

3.6 设计科学合理的网站检查方案

高校信息化建设进程中保证信息安全还应该对网站的检查方案实现科学合理的设计。对网站进行定期的安全检查，最主要的是要对检查的具体范围要予以确定[4]。在我国高校大力推进数字化校园建设的现阶段，其内部网络的应用服务也越来越多，所对应的管理方式也有所不同，因此针对高校的实际发展情况，应该对网站信息安全的检查范围实现确定，保证检查不会出现遗漏；另外，还需要对检查的方向予以确定，使得检查工作更加具有针对性，严格按照信息安全检查制度予以落实。

3.7 优化技术选择

根据实际需要引入先进的身份鉴别机制、访问控制技术、加密存储传输技术、审计跟踪技术、病毒查杀技术等措施，形成一个包括实体安全、数据安全、软件安全、网络安全、运行安全等在内的相对统一、强度均衡、全面完整的安全防护体系。此外，高校档案部门还应高度重视相关工作人员的保密技能培训，重点引进和培育具备计算机基础的复合型档案保密人才。

3.8 定期评估，强化访问控制

信息技术发展日新月异，安全防护软件系统因为其复杂性，所以在具体研发中难以避免地出现各种问题，造成安全防护系统漏洞，较难有效地防御信息安全威胁[1]。因此，高校应该合理引入信息安全风险评估机制，定期或者不定期地对网络安全情况进行全面风险评估，找出薄弱点，然后采用合适的措施进行强化，以便有效降低信息安全风险。除此之外，还应该注重对存储设备的安全管理，增强访问控制。在此过程中，相关方面可以限制可移动储存设备及结构，避免不法分子借助硬盘、软盘等窃取信息。同时，还可以将共享设置直接禁用，避免通过手提电脑等进行信息的窃取。对于用户访问网络资源的权限也得加强控制，具体可以实施层次授权制度。

3.9 信息加密和认证权限

信息加密技术是保证信息安全的有效方式之一，一方面能够有效的防止非授权用户的搭线窃听和入网，另一方面还能够有效阻止恶意软件的攻击。对网络信息进行加密的主要目的是对高校内部网络的口令、数据文件和控制信息实现有效的保护，避免网络信息系统受到恶意的攻击。应用加密技术能够将重要且敏感的信息内容转换成为很难读懂的乱码性信息，从而实现保护信息安全的目标[2]。除了信息加密技术，认证权限也是提高信息安全的重要手段，主要针对的是越权访问；借助认证权限技术，用户在对系统进行访问的时候，需要输入口令进行身份验证，当用户身份确定之后才允许进入系统，并对具体的操作进行了限制，反之系统将会对该用户的请求实现自动拒绝。

3.10 防火墙的安装

防火墙技术是现阶段我国高等院校信息化建设进程中对信息安全予以保护的主要手段，防火墙技术能够实现高校内部网络系统及其外部网络系统之间的相互隔离，在二者之间构建唯一的通道，且数据信息的传输和访问都必须通过该通道来实现，从而对高校的内部网络实现保护。在校园网的边界处设置网络防火墙，对外部网络对内部网络的访问实现控制是我国高等院校保护信息安全的主要措施之一，当然，仅仅只是依靠防火墙技术对信息安全加以保护还远远是不够的，还应该进一步加强对网络信息安全保护的教育，并提高防范技术措施的先进性和主动性[3]。

结语：

综上所述，随着计算机信息技术的进步，造成了许多的安全隐患，因此需要依据现实的情况，从内部管理以及信息安全这两个方面进行深入研究。同时高校的信息化建设还应以信息技术为根据，如此才能够增强学校内部的信息技术管理体系，及时做出应对措施从而有效防范学校中信息网络的安全不受侵害。

参考文献：

[1]梁伟雄.高校信息化建设进程中信息安全问题及对策分析[J].佳木斯职业学院学报，2021，37（7）：107-108.

[2]杨振宇.高校信息化建设进程中信息安全问题及对策分析[J].电脑知识与技术，2020，16（16）：68-69.

[3]刘成榆，赵卫.高校信息化建设进程中信息安全问题成因及对策分析[J].教育信息化论坛，2019（02）：98-99.

[4]郭庆贺，吕春雁，贺春亮.高校信息安全保密管理中需要注意的问题[J].现代信息科技，2019（21）：151-152.