ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.17, No.16 June 2021

E-mail: jslt@dnzs.net.cn
http://www.dnzs.net.cn
Tel:+86-551-65690963 65690964

数字化校园网络安全防范机制构建及实践分析

苏治中

(广州开放大学,广东 广州 510091)

摘要:在信息技术和大数据技术发展的今天,数字化校园建设已成为社会上广泛关注的问题,一些学校为了谋求自身的稳定性发展,开始加强了对数字化校园网络建设的重视程度,实现了硬件资源和软件资源的优化性配置。但是由于整个网络虚拟性特征和不确定性因素较多,很容易出现一些安全隐患,不仅会造成严重的信息泄露问题,还会使整个校园网络出现瘫痪的情况,因此在实际工作中需要加强对数字化校园网络安全防范机制构建工作的重视程度,根据数字化校园网络的特点来提高后续工作针对性。

关键词:数字化校园网络;安全防护;机制

中图分类号:TP393 文献标识码:A

文章编号:1009-3044(2021)16-0040-03

DOI:10.14004/j.cnki.ckt.2021.1756

开放科学(资源服务)标识码(OSID):

The Security Prevention Construction and Practice Analysis for Digital Campus Network

SU Zhi-zhong

(Guangzhou open University, Guangzhou 510091, China)

Abstract: which will not only cause serious information leakage problems, but also paralyze the entire campus network. Therefore, it is necessary to strengthen the importance of the construction of the digital campus network security prevention system, and improve the pertinence of follow-up work according to the characteristics of the digital campus network

Key words: campus digital network; security; mechanism

在实际数字化校园网络安全建立过程中,需要进行硬件系统和软件系统的不断融合,防止一些重要数据出现破坏和泄露的问题,因此在实际工作中需要加强对网络安全防范机制构建工作的重视程度,最大限度的保护校园网络中的一些信息。

1 数字化校园和网络安全的特点

在进行数字化校园网络安全防范机制构建时,需要加强对数字化校园和网络安全特点了解以及认识,从而为后续工作奠定坚实的基础。数字化校园网络主要是充分的发挥计算机技术优势,对学校进行教学管理和教学科研的有关服务,并且还要对相关信息资源进行多方位的整合,实现数字化的管理过程。通过数字化的管理不仅可以将学校信用资源进行全面的整合,还有助于实现用户的统一性管理和协调,共同的推进数字化校园网络建设工作的有序进行[1]。在信息化时代,网络安全构建变得越来越重要,不仅仅包含了有关网络技术和计算机科学方面知识,还包含了有关数学和服务方面的综合技术,这在一定程度上也增加了网络维护和管理难度。计算机在校园工作中的作用越来越突出,但是由于整个网络环境是非常复杂的,很容易出现信息分布不均等问题,再加上各个信息具备互联性和开放性的特征,如果在某一个节点处出现信息泄露和丢失问题的话,那么会使得其他信息在运用过程中也存在着较大的泄漏隐患,增加了实际网络安全的发生概率。因此在实际工作中需要加强对数字化校园建设和网络安全管理的维护力度,从而满足学校当前管理的需求以及管理要求。

2 数字化校园网络安全的隐患

在我国经济发展的进程中,我国科学技术手段也在不断地更新和进步,经过多年的网络建设和信息技术水平的提高,各个学校纷纷建立起了数字化的校园来支撑实际教学和管理工作的有序进行,推动了我国教育事业的不断进步。在当前大多数学校都建立了自己独特性的校园网络,并且实施了数字化的教学管理,从而使得学校教学管理效率能够有高效提高。但是随着信息技术的不断发展和深入,网络安全问题接踵而来,使得实际学校管理的效率和水平无法得到提高。如果在网络信息上出现泄漏问题的话,那么会影响实际科研活动和教学管理活动的有序进行,因此需要深入的分析存在于当前校园网络中的一些安全隐患,提出有效解决措施,从而推动数字化校园网络的不断发展。从整体上看数字化校园网络安全隐患主要分为以下几个方面:

2.1 管理方面的漏洞

1)管理内容的繁杂

在数字化校园网络中,每一个教师和管理人员都是网络中的重要主体,在实际管理工作中需要根据这些主体的组成部分实施科学性的网络管理方案,从而使得实际校园网络能够平稳

收稿日期:2021-03-10

的运行。在当前数字化校园网络管理中还存在诸多漏洞，主要体现在是对用户群体的管理上，由于学校是教师和管理人员所组成的庞大群体，一些学校在进行数字化校园网络建设时，并没有加强对管理制度有效优化，也没有融入身份认证系统，使得实际安全防范机制无法在实际中发挥其应有的价值和效果。这就导致了一些内部管理人员在登录到学校内部的网站时，并没有设置专业性的用户名以及密码等等，一些重要的信息没有经过严格的审核就传播给外部人员和学校内部的无关人员[2]。不仅会使得信息的储存效果无法得到有效提高，还会给后续信息使用带来诸多的困扰以及难题。在此基础上一些网络罪犯侵入到电脑系统中，随意传播一些重要的信息，或者是在学校网站中融入一些不健康的信息，对数字化网络的维护带来诸多的困扰以及难题。

2)设备的落后

其次，一些学校的电脑设备是太过陈旧的，在网络设备安全配置方面还存在着不足的问题，由于各个系统存在着滞后性的特征，整个管理工作较为松散，使得整个数字化校园网络处于开放的状态中，再加上一些管理人员并没有加强对这一网络维护工作重视程度，使得这一网络长期处于开放的环境中，严重影响信息储存工作效率的提高，使得数字化校园网络建设存在诸多的不足。由于在网络管理方面出现较为松散的困扰，导致一些学校的安全预警手段无法在实际中发挥其应有的价值和效果，在防范上也存在诸多的困难。在这一背景下，校园网络中的疏忽和漏洞越来越多，不仅无法解决存在以往网络运行中的一些问题和安全隐患，还很容易加大危害发生的概率和严重程度，使得网络管理效果和水平无法具备与时俱进的特征，在应用时也会存在诸多的困扰。

2.2 校园内部存在的隐患

在当前数字化校园网络运行过程中，在校园内部的隐患也是比较突出的问题，比如一些学校的学生刚刚学习了有关计算机方面的操作，所以跃跃欲试，开始对学校的网络产生一定的想法。另外这部分学生对任何事件都充满了好奇心和求知欲望，很容易由于非主观性的因素而出现校园网络使用的故障，因此在实际工作中需要加强对这部分学生的思想政治教育力度，向学生讲解网络安全的重要内容，从而提高实际校园网络安全管理效果和水平。与此同时校园内部的计算机病毒和网络病毒也是存在于内部隐患中的问题，随着我国当前网络技术的不断发展，计算机病毒逐渐朝着对外线的方向而不断发展，甚至是一些病毒还存在着隐蔽性的特点，整个网络环境是非常复杂的[3]。如果在实际网络使用时，一些使用终端随意让各种木马病毒侵入的话，那么整个网络会出现多种多样的入侵，造成严重的瘫痪，使得实际校园网络安全管理效率无法得到有效提高。

2.3 外部隐患

外部隐患是由于计算机本身具备开放性和通用性特点而决定的，校园网络一般是和外部网络相连，如果外部网络出现破坏的话，那么会影响校园网络本身的安全性。比如来自外部的隐患没有访问的授权，但是如果这一访问本身就带有病毒的话，那么会在短时间内传送到校园网络的内部，无法保证校园网络的平稳性运行。另外一些外部网络本身还存在一些不安全的隐患，和网络之间的协议存在着一定的矛盾，这些都会使得网络出现堵塞和拥挤的问题，甚至还会由于病毒的入侵产生重要信息丢失的问题，限制了网络安全效率的提高。

以上就是存在于当前数字化校园网络中的一些安全隐患，在实际工作中加强校园网络安全管理是非常重要的，因此需要相关管理人员加强对数字化网络安全的了解和认识，明确校园网络的特点，制定有效的防范措施，并且还需要对以往的安全防范模式进行不断调整和优化，从而更加贴合于学校当前网络安全管理的要求以及标准，提高网络安全管理的效果和水平。

3 数字化校园网络安全防范机制构建的策略

3.1 安全防范思路

在进行数字化校园网络安全防范机制构建时，需要加强对安全模式的合理性利用，从而使得这些安全模式能够在实际中最大限度地保护信息的不泄露和不丢失，并且还可以对一些安全隐患起到重要的抵制效果，从而不断地提高数字化校园网络安全防范的效果和水平，从整体上看，在模式构建时要分为以下几个方面：

1)设备

在进行网络安全防范机制构建时，加强设备的融入是非常重要的，需要从设备安全保护的角度上充分的发挥网络安全预警机制的效果及作用。设备安全属于网络防范体系中的重要组成部分，并且也是提升网络安全运行的可靠落脚点，在实际工作中包含的是网络互联设备和其他工作站的设备，学校管理人员需要加强对设备和资金的投入力度，通过教学管理工作的优化和管理模式的调整利用相关设备来实现此功能。另外还需要特别注意设备的安全性以及可靠性，这也是校园网络系统正常运行的重要基础和因素，相关学校领导们可以适当地借鉴其他学校在设备融入方面的一些经验，再结合学校当前校园网络管理的要求和标准融入先进的设备，从而提高设备型的效果和水平。

2)管理

除了要融入先进的设备之外，还需要进行科学而完善的安全管理工作，从而保证数字化网络安全效率的提高。在实际工作中管理，在校园网络安全性保障具有重要的意义，对于规模较大的校园网络来说，维护人员要明确主要的工作要点，定期对系统进行科学性的维护，从而保证系统的安全和平稳运行。相关学校可以开展定期地组织培训活动，从而不断增强这部分工作人员的工作积极性以及工作热情，更加有条理和全面的进行数字化校园网络安全的管理。大多数学校将系统维护人员进行安全培训中可以结合系统在运行时的一些问题进行深入的探讨以及研究，从而不断地增强相关人员的应急处理能力以及工作能力。通过网络安全性的管理，能够使相关操作员更加规范性的利用校园网络来支撑实际工作有序进行，也有助于使网络系统运行能够具备安全性和合理性的特征，因此在实际工作中需要加强对管理工作的重视程度。

3)预案

在进行数字化校园网络安全管理时，还需要提出紧急预案，从而灵活的应对在网络运行中的一些安全问题以及困扰。在实际工作中需要结合以往的工作经验，对很有可能发生网络安全突发情况进行紧急预案的制定，从而提升网络安全管理效果和水平。相关管理人员可以对网络安全等级进行科学的划分，并且贯彻落实安全责任制度，根据不同的事件来提出有效的解决措施，并且还要运用关键网络安全维护技术以及设施从而减少危害事件发生的概率。在实际工作中，对于局部和小范

围的安全事件来说，需要融入防火墙技术，从而对病毒起到重要的抵抗和消除作用。对于突发事件来说，需要设置不同的处置措施和处置方法，这样一来当安全事故发生之后，各个部门之间可以临危不乱，相互合作，有序地解决在数字化校园网络中的一些安全问题，为后续的处理工作奠定坚实的基础。

4）技术的利用

在数字化校园网络安全防范机制中，还需要加强对安全技术的科学性利用，从而提升网络安全管理的效果和水平，在实际工作中需要认识到数字化校园网络安全威胁的复杂性特征，在应对外部安全威胁时，要采取防火墙技术，对内部网络进行威胁防范时，可以约束上网行为构建完善的管理系统。相关学校还需要加强对设备和资金的投入力度，可以购买漏洞扫描系统和入侵防御系统等等，更多的加强校园网络安全管理的力度。为了提升实际网络安全管理效果和水平，可以对整个校园网络进行层次性的划分，以多种网络安全技术作为主要的技术实现立体性和多样性的防护体系，从而使得数字化校园网络安全防范效果和水平能够全面提高。

3.2 网络安全模型的选择

1）IATF模型

在这一模型实施过程中，可以从整体性和过程性的角度，对安全问题进行全方位的分析，查找出最为本质性的安全隐患。在实际工作中要采取多层次和深层次的安全措施，来保证信息系统的安全，并且将网络边界和计算环境进行相互的融合，以支撑体系作为主要的基础，从而提升网络安全管理效果和水平。在模型构建时，需要通过模型偏重的技术手段来构建完整的信息安全体系，在构建时要将数字化技术和操作进行相互的融合，从个体性的角度充分的发挥系统应用的功能以及作用，从而最大限度地保证系统的安全。

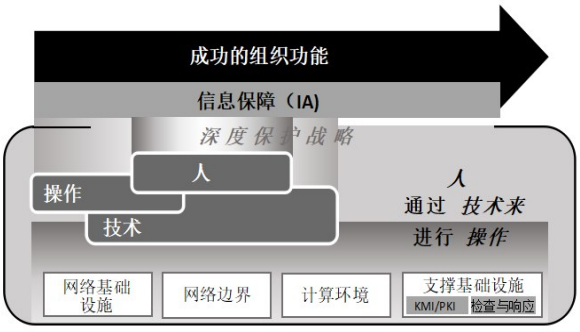

图1　IATF模型

2）CNATF模型

在这一模型实施的过程中，需要做好设备和管理模式的充分性，从而充分的发挥设备的功能以及优势。在实际工作中，由于设备安全是处于最内层的，也是整个系统运行的核心点以及落脚点，因此需要通过网络互联体系保证各个服务器和工作站的平稳性运行。另外还要使得最终最底层的设备能够具备安全性和可靠性的特征。其次在管理方面由于整个校园网络的用户全是比较庞大的，因此如果在某一个安全管理中出现偏差的话，那么会影响整个系统的平稳性运行，因此在实际工作中需要通过设备的安全性管理，贯彻落实安全责任制度，从而保证系统平稳性运行。

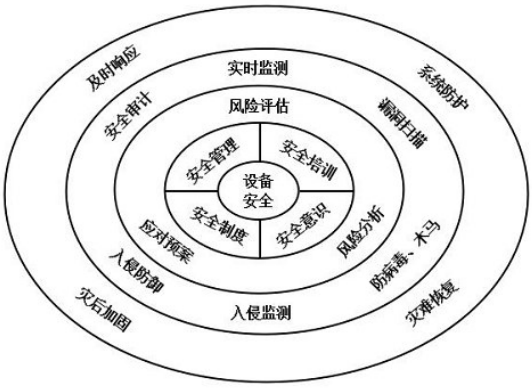

图2　CNATF模型

4 结束语

在进行数字化校园网络安全防范机制构建时，需要在以往安全防范机制的基础上实现有效的创新以及发展，并且还要做好设备的维护以及管理模式的优化性调整，加强技术和设备的投入力度，结合数字化校园网络安全防范机制构建的要求和标准制定紧急预案，从而使得使数字化校园网络中的安全隐患能够得到有效的解决，提升系统运行的效果。

参考文献：

[1] 杨峻楠,张红旗,张传富,等.基于不完全信息多阶段博弈的入侵路径预测[J].计算机应用研究,2019,36(2):519-524.
[2] 王骏.计算机信息管理技术在网络安全中的应用[J].电子技术与软件工程,2018(2):203-204.
[3] 闫萍.计算机信息管理技术在维护网络安全中的应用策略探究[J].通讯世界,2017(21):77.

【通联编辑：代影】