浅析开放大学计算机网络安全及防范策略

王毅凡

(国家开放大学实验学院,北京 100081)

摘 要:近些年来随着网络技术的不断发展,网络安全问题逐步的暴露出来。网络安全是开放大学进行信息化建设的重要基础,而对于这么一所学生众多,利用信息化技术为支撑的学校,网络安全的问题更是不容小觑。文章从网络安全的角度出发,对其影响的因素进行了分析,在此基础上综合现在技术手段和实际情况,有针对地提出网络安全管理手段。

关键词:开放大学;网络安全;管理手段

中图分类号:TN915.08 文献标志码:A 文章编号:2095-2945(2017)35-0132-02

随着网络大数据时代的到来,网络信息技术高速的发展进步,不仅给人们生活和工作带来了很多便利,甚至在教育领域也开始发挥日渐重要的作用。国家开放大学正是在教育部支持下,以现代信息技术为支撑,面向成人开展远程教育,是一所没有围墙的中国式开放大学,它的主要任务之一是探索现代科技与教育的深度整合,促进、引领教育信息化和教育现代化,特别强调要充分利用现代信息技术手段,整合、利用社会优质教育资源,促进教育公平,提升教学质量和管理水平,迄今为止在校生高达 300 多万。

1 开放大学网络安全防护的重要性

随着国家开放大学学生学习过程和教学资源等重要数据的日益增加,面临的数据安全问题也越来越紧迫,一旦出现疏忽,给不法分子以可乘之机进行网络攻击,造成数据被肆意篡改、非法访问,不仅会给个人带来损失,甚至会造成网络系统崩溃等重大安全事故,后果十分严重,做好开放大学的网络安全防护工作已经迫在眉睫。

2 网络安全的影响因素

2.1 网络安全存在漏洞

目前大多数的计算机网络传输协议都是 TCP/IP 协议,国家开放大学的网络也不例外,由于协议最初设计的时候只考虑到传输的可靠性即能不能完整的收发,而没有考虑安全问题,导致在安全问题上就有先天缺陷,因此使得国家开放大学在网上传输数据时面临着各种安全问题[1]。国家开放大学实行的是分级办学,分级管理的办学和管理模式,一共分为四级,总部、省校、分校和学习中心。其管理系统众多,招生管理系统、教务管理系统、考务系统等也同样不完善,存在或多或少的安全漏洞,使得计算机网络时时刻刻处于高危状态。上述管理系统大部分都部署在 44 所省校的机房内,分校和学习中心只有访问权限,因此省校的网络安全显得更为重要。

2.2 设备更新、管理不到位

国家开放大学的计算机网络数据的传输必须通过各个设备的协同配合,缺少任何一个网络安全都无法保障。在基层的一些学习中心,由于资金有限,网络安全设备更新速度跟不上,导致抵抗外界网络攻击的能力较低。对于经济发达的地区,存在对网络安全重视程度不够,网络专业技术不达标的情况,未能通过已有的硬件设备进行有效的网络监管,因此也面临着较大的网络安全问题。多级办学的模式虽然给学生创造了学习的便利,但也导致了服务器等硬件众多且分布比较广,增加了数据传输的风险性。

2.3 外部病毒入侵

对于国家开放大学来说,病毒入侵是最应该注意的影响网络安全的因素。病毒根据破坏性可以分为非破坏性攻击和破坏性攻击两类,前者目的是为了扰乱系统的运行,后者是为了进行数据盗取和破坏等非法行为,计算机一旦被病毒入侵,由于病毒易多发和易传染的特点,计算机在任何场所和任何时间都可能会被破坏。如果计算机被病毒入侵,学习者的学习数据、考试数据、收费数据等重要信息都会被不法分子掌握,造成不可估计的严重后果。现阶段,系统管理人员会利用第三方杀毒软件定期地在服务器上进行病毒的查杀和漏洞的修复,暂时没有掌握主动入侵检测技术,未能对当前网络系统进行网络安全性评级,自主抵御病毒入侵的能力还不够。

2.4 安全意识欠缺

国家开放大学的任课老师和管理人员大部分没有相关计算机网络知识,也没有接受过计算机安全培训,安全保密意识不强,很容易将自身的计算机登录账号和国开相关系统的入网账号与他人共用,过后也未及时修改密码,使得用户口令泄露,造成潜在安全隐患[2]。此外系统管理员的访问权限过高,在国开的相关管理系统当中,管理员账号权限能对数据库后台的所有记录进行直接操作,如果系统管理员账号一经被盗,没有第二道防线,后果非常严重。现在国开及省校管理员系统学习组织培训力度不够,由于系统众多,很多管理人员不熟悉操作规程,这很有可能引发重大事故,使信息无法挽回地丢失。

3 开放大学网络安全管理对策研究

3.1 加强制度保障和人员管理,组织系统相关培训

对特别重要的岗位要实行多人负责制,任何人不得拥有过大的访问权限。管理员要明确自身岗位职责,做好自身权限范围内的工作,保障管理区域网络的安全。同时还要制定服务器和相关管理系统的管理制度,明确用户访问权限,不随意多开账号。

针对于国家开放大学的教师和管理人员,学校应经常组织网络安全培训,加强相关人员计算机网络安全意识。在日常工作中设置复杂的密码在一定程度上可以保护重要信息,并做到不与别人共享密码,定期修改密码口令,不随意打开不安全网站、不接收恶意文件、不执行不明程序等操作。对于自己的计算机要定期的进行病毒查杀,维护系统漏洞。针对于学校内网络保障部门,必须注重提高内部计算机管理人员的网络安全意识,注意采用适当的方法去培养一批具有专业计算机技术的网络监控人员,打造属于国开的计算机安全管理团队,能及时对网络不法攻击做出处理,构建一个系统全面的计算机网络安全管理体系,致力打造一个安全可靠的计算机网络环境。

3.2 划分 VLAN,绑定 MAC

为了便于管理和安全,对于国开单位内部的网络在不同区

(下转 134 页)

作者简介:王毅凡(1991-),男,汉族,硕士研究生,现从事国家开放大学实验学院教务系统研究与运维工作。

及管理人员应当加强对山区、隧道地区接触网设备零件的检修和分析，要区别对待此处接触网与普通地段接触网，缩短定期检查日期，采用先进的检测、检修仪器，加强对接触网各零部件的检测和维护。

4.2 接触网绝缘子预防污染物（污闪）的措施

接触网绝缘子污闪情况容易发生在每年秋末冬初和冬末春初两个时节，这与空气中污染物数量与潮湿情况直接相关。秋天多雾，尤其在凌晨期间容易产生过多潮气，使灰尘附着在接触网设备上[4]。冬末，雨雪情况减少，此时多为大风天气，灰尘、杂物混着在空气中，成为污闪发生频率较高的时节。对此，各地区应当根据实际情况采取不同的污闪防治措施。例如，在靠近北方地区，可以通过增加绝缘子的爬电距离，提高绝缘水平。此外，维护人员应当及时对绝缘子进行清扫，通过定期清洁减少污闪发生的机率。在后期维护中可以针对重点污闪易发区涂抹防污涂料，像有机硅、石蜡等材料都可以起到防尘作用。

4.3 接触网异物源预防措施

由于铁路牵引供电接触网建设是随铁路建设而架设的，因此在沿线建设过程中不可避免的会面临各种异物源，这使得接触网运行环境中始终面临不可控的风险。对此，设备管理单位应加强对当地接触网设备的巡视和管理，建立详细准确的台账，提前预防异物源干扰问题的产生。对于铁路单位无法解决和控制的异物源应积极寻求地方政府的协助。

当异物已经出现在接触网设备上时，需要供电设备管理单位立刻采取应急措施。当较小异物在接触网设备上漂浮或者简单缠绕时，工作人员可以在线路封锁状态下，利用绝缘工具清除异物；而当异物与接触网设备严重缠绕或异物长大时，则需要进行停电、封锁线路处理。

4.4 铁路上跨桥、危树风险预防措施

做好设计源头管理。在建设上跨铁路的各类桥梁时应避免在桥梁外侧悬挂各类附属物，从源头上做好卡控。对于必须设置的防抛网则应选择耐腐蚀、制作工艺优良的材质，延长使用寿命。

铁路危树的风险消除。随着邻近铁路发生倒树影响供电和列车运行事件的增多，铁路在建设初期即增加了对危树等外部环境的排查和治理。彻底解决危树隐患必须从设计和施工源头进行防范，如：在建设征地时应考虑对倒伏范围内的树木进行清除。对既有历史原因形成的危树隐患，铁路局和地方政府形成处理的联动协调机制，制定费用支出原则等，共同预防倒树发生。

5 结束语

总之接触网设备是保证牵引供电系统维持正常运作的关键设备，要保证接触网设备的正常运行，就必须做好供电设备运行环境安全风险管理。对于电气化铁路牵引供电系统而言，接触网设备运行环境中存在的风险问题必须重视，未来相关管理人员应当继续加强对接触网建设技术、接触网绝缘子污闪防治、接触网异物源等外部环境隐患预防等内容的研究，为接触网设备创造安全、稳定的外部运行环境，促进牵引供电系统的安全、可靠运行。

参考文献：

[1]何彦.牵引供电调度安全运行管理工作的几点建议[J].科技展望，2016（23）：198.
[2]张鸿玉.牵引供电调度如何做好安全运行工作[J].科技风，2013（11）：200–201.
[3]程宏波.计算及不确定性的牵引供电系统健康诊断及风险评估方法研究[D].西南交通大学，2014.
[4]许龙.基于设备维修策略的接触网管理信息系统的研究[D].西南交通大学，2013.
[5]姚凌云.浅议提高供电系统设备管理水平的措施[J].科技创新与应用，2016（27）：221.

（上接 132 页）

域划分 VLAN，并设置访问权限设置，防止国开内网某一网段的用户在受到病毒攻击后，将病毒扩散至其他网段的用户，从而造成网段堵塞，或者造成病毒伪装源地址进行网站攻击的情况，带来极坏的影响[3]。国开应当建立信息系统网络安全访问路径，采用路由控制的方式，来确保客户端与服务器之间的安全连接，对于不同业务部门根据工作内容、保密敏感性等因素进行划分不同的网段，特别是网络安全保障部门以及应进行 IP 与 MAC 绑定，避免遭到 ARP 欺骗攻击。在重要的数据库服务器上部署入侵检测系统，对蠕虫攻击、缓冲区溢出攻击、木马攻击、端口扫描等恶意操作进行监测，将攻击发生的时间、类型以及攻击源 IP 等信息详细的记录下来，提供给网络安全部门。

3.3 采用 VPN 技术构建虚拟网

VPN 技术指的是运用加密解密技术和隧道技术在公共网络中远程连接多个内部网络，并通过网络数据的相关技术为用户建立安全的传输通道，在使用上具有成本低、灵活性强等特点，能进行大容量扩充，服务保证性强。使用虚拟专用网的用户可以掌握自身网络的控制权，对于网络的安全设置和管理权限都可以自由设置，很大程度上限制了外来非法访问几率，保证了国开网络的安全运行。国开网络管理人员还可以通过 VPN 服务器来构建内部虚拟专用网，只有得到访问权限的用户才能进行 VPN 服务器连接并获得某些信息的访问权，从根本上拦截外部非法访问。由于 VPN 服务器和客户机之间的通讯数据都进行了加密处理，在 44 所省校与总部进行学籍信息，招生信息，收费信息等重要数据交互时，通过 VPN 构建的虚拟专用通道更加可靠。

3.4 身份认证技术，采用 key+口令方式

身份认证即对访问网络的合法用户鉴别，确保合法用户能正常使用网络，防止非法用户攻击网络，保证网络的安全性。身份认证的重要性合法用户一般都具有两种身份，一种是物理身份和数字身份，身份认证就是对这两种身份是否一致进行鉴别。国开的管理系统当中，应当引入身份认证技术的理念，对于存储着学生、教师和管理人员的大量数据的核心数据库的管理操作，应当采取 key+口令的方式，key 由网络安全管理部门统一派发，并且只有一个，无法复制，确保 key 的唯一性，并且要随机设置口令并定期更换。此外，为了保障核心数据库的数据安全，在重要业务岗位，例如学生成绩录入、信息和数据库管理等，不同岗位对数据库的访问权限合理控制，保证正常地开展工作。

4 结束语

在数字化时代下，要确保其网络安全，才能保障国开远程教育的正常运转。因此国家开放大学应当从管理层面、技术层面出发，搞好自身的信息安全建设，防止网络系统受到破坏，保障整个系统的整体高效稳定的运行，更好的为全国师生提供优质的服务。

参考文献：

[1]邹佳顺.云计算环境下安全问题及其对策研究[J].计算机光盘软件与应用，2012（14）.
[2]王秀翠.数据加密技术在计算机网络通信安全中的应用[J].软件导刊，2011（03）.
[3]李林，杨勇.计算机网络安全漏洞防范策略探析[J].电子技术与软件工程，2016（12）.
[4]张志华.新时期计算机网络安全风险及策略研究[J].科技创新与应用，2013（13）：72.