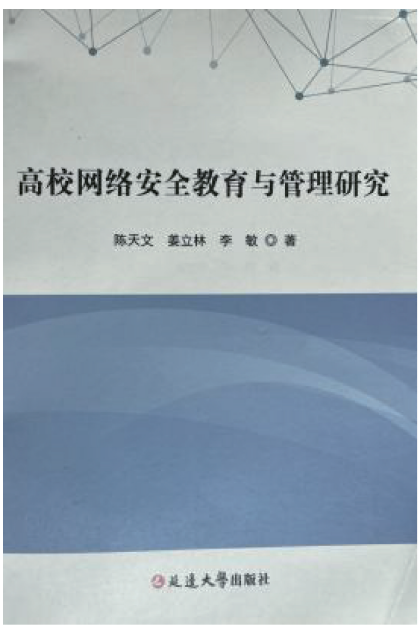
高校计算机网络安全教育管理策略
——评《高校网络安全教育与管理研究》



书名:高校网络安全教育与管理研究
作者:陈天文,姜立林,李敏
出版社:延边大学出版社
ISBN:9787230022446
出版时间:2022年3月
定价:50元

在数字化浪潮席卷全球的今天,高校早已不再是象牙塔里的封闭学术孤岛,而是成为了国家关键信息基础设施的重要组成部分。随着智慧校园、科研云平台以及物联网的深度渗透,高校网络承载着海量的高精尖科研数据、师生个人隐私以及核心教学资源,其开放性与高价值性使其沦为黑客组织、勒索软件乃至境外某些国家或组织持续性威胁入侵攻击的"首选靶场"。面对日益狡黠且自动化的攻击手段,传统的"防火墙+杀毒软件"式粗放管理已彻底失效。高校计算机网络安全教育与管理,必须摒弃形式主义,构建一套立体化防御体系,这不仅是保卫校园稳定的底线,更是护航国家网络空间主权的战略必然。

数字化时代,高校网络早已不仅是教学科研的辅助工具,更是承载办公自动化、教务管理乃至意识形态传播的"数字底座"。然而,当师生享受便捷时,病毒攻击、系统漏洞、投入不足等隐患如影随形,时刻威胁着这座"象牙塔"的安宁。《高校网络安全教育与管理研究》一书为高校管理者开出的一剂"良方"。全书摒弃空洞的理论堆砌,构建"基础-教育-管理-创新"的闭环逻辑。全书共4章,第1~2章夯实理论地基,剖析了网络环境下的安全体系与防护技术,以及高校网络安全教育创新;第3章直击痛点,针对大数据、新媒体时代大学生群体的行为特征,提出了破解安全教育"入耳不入心"顽疾的创新策略,强调从"被动防御"转向"主动引导"。尤为值得称道的是书中对具体场景的深耕。作者没有停留在泛泛而谈的管理制度上,而是将镜头推向了图书馆、机房、计算中心、招生系统等高频风险区。特别是对"高校网络意识形态安全体系"与"大规模无线网实施"的探讨,切中了当前高校管理的命脉。第4章不仅分析了高职校园网用户量大、活跃度高带来的管理难题,还结合计算机信息技术的实际运用,给出了招生信息管理、教务系统防护的具体对策。总体而言,这本书跳出了纯技术视角的窠臼,将技术防护、制度管理与育人理念有机融合,为构建清朗、安全的智慧校园提供了有力的智力支撑。

目前亦有部分高校的网络安全教育尚停留在"合规层面",即基于课程学分要求,并结合相关政策要求,开设一门选修课,通常以网课形式开展具体教学活动,以理论学习为主,目的是让学生掌握相关基础理论知识,并能够顺利拿到学分。这种"应付式教学方式"导致的结果是,学生可能背得出《网络安全法》的条款,却分不清钓鱼邮件和正常通知的区别,甚至为蹭免费VPN主动把设备置于高危环境中。真正的高校网络安全教育重构,必须打破"计算机学院独奏"的局面,转向"全学科共鸣"。首先,内容的去理论化是关键。现在的00后、05后学生是数字原住民,他们不需要被科普"什么是互联网",他们需要的是"在这个场景下我该怎么做"。如针对文科学院,不要讲复杂的加密算法,要讲如何识别针对大学生的兼职刷单诈骗、人工智能换脸诈骗的技术原理和心理陷阱;针对理工科,则要深入代码审计、漏洞挖掘,但必须加入"白帽子"伦理教育——技术无罪,但使用技术的边界在哪里。其次,实战化演练要成为常态,而非"表演"。很多高校的夺旗赛比赛只面向特长生,普通学生只能当观众。学校需要建立分级的试验环境。低年级可在模拟沙盘里体验"中病毒后电脑被锁"的恐慌,高年级则直接参与学校真实系统的"众测"。如让学生在受控环境下尝试攻击学校的选课系统(当然是在教师监控下),让他们亲身体验SQL注入带来的后果。这种"痛感教育"比一百次说教都管用。当学生发现自己随手写的一行代码就能导致数据库瘫痪时,安全意识才会真正形成肌肉记忆。最后,评价体系要动真格。现在的安全教育考核往往是一张卷子定生死。应该引入"行为积分制",将日常的安全习惯纳入学分或综合测评。

如定期发送模拟钓鱼邮件,点击链接的学生扣分,主动举报的加分;发现公共机房漏洞并报告的,给予创新学分。让安全表现直接挂钩利益,学生才会真正上心。

笔者认为,在高校的行政架构中,网络安全管理往往是个“踢皮球”的重灾区。信息化中心负责技术运维,学工处负责学生管理,保卫处负责物理安全和案件侦破,教务处负责教学安排。结果就是,技术部门不懂学生心理,学工不懂技术风险,保卫处不懂电子取证。这种割裂导致响应滞后——往往是学生被骗了钱、数据泄露了,几个部门才坐到一起开会,此时损失已经无法挽回。要改变这种状况,必须建立一种“扁平化、融合式”的协同机制。核心在于建立一个实体化的“网络安全应急响应中心”,但这个中心不能只由网管员组成,必须吸纳学工辅导员、保卫干部甚至法律顾问。这个机构的职能不是“管”,而是“服务”和“处置”。如当监测到某个 IP 地址在大量扫描校内端口时,系统应自动报警,技术人员立即定位到具体宿舍,学工辅导员同步介入。这时候不是直接断电断网惩罚,而是先谈话教育,了解学生是在挖矿还是在做试验,或是中了木马。这种“技术+行政”的组合拳,既有威慑力又有人情味。此外,管理的触角要延伸到“灰色地带”。现在的学生善于利用技术手段绕过监管,如使用私搭的代理服务器、破解版软件,甚至在校内网络进行 P2P 下载,这不仅占用带宽,更是病毒传播的温床。管理部门不能简单地“一刀切”封堵,而要通过流量分析找到需求背后的痛点。如果学生是因为正版软件太贵而用破解版,学校是否可以提供廉价的正版化服务? 如果是因为内网速度慢而用 P2P,是否该升级基础设施? 管理不仅是约束,更是疏导。通过解决学生的实际困难来降低安全风险,这才是高水平的管理智慧。还要特别重视“人防”中的关键节点——导师制。在研究生阶段,导师对学生的约束力往往超过辅导员。必须将网络安全责任纳入导师的考核体系,明确导师对学生使用科研算力、处理敏感数据的监管责任。很多实验室的服务器被黑客控制变成“肉鸡”,往往是因为学生为了图方便设置了弱口令,而导师毫不知情。把导师拉进安全管理的链条,就可补上了高校安全最大的一块短板。

技术和制度是硬约束,文化则是软实力。在一个健康的网络安全生态中,不安全的行为应该像在公共场合吸烟一样,被视为不文明行为甚至被排斥。首先,高校要做的是“去神秘化”,网络安全不应该是黑客电影里的酷炫代码,而应该是像“饭前便后洗手”一样的日常习惯,这需要持续的、高频次的“微宣传”。不要只在每年 9 月的“网络安全周”挂横幅,而是要把宣传做进食堂的餐垫上、做进快递取件码里、做进校园网的登录弹窗里。如在登录界面显示“您上次登录是在异地,请确认是否本人”,这种潜移默化的提示比讲座更有效。其次,培养“吹哨人”文化。在传统观念里,发现漏洞往往被视为“找茬”或“捣乱”。高校要旗帜鲜明地鼓励“白帽子”行为,设立专门的漏洞奖励计划或安全建议奖。哪怕是学生发现了官网的一个错别字或死链,只要涉及安全隐患,都应该给予精神和物质奖励。要让学生觉得,帮学校找漏洞是一件很酷、很光荣的事,而不是会被记过处分的风险行为。当每个学生都成为网络安全的“流动哨兵”,黑客的攻击成本将呈指数级上升。然后。关注“人”的心理防线。大量的网络安全事件源于内部人员的情绪宣泄或无意疏忽,如毕业生因为离校手续不满而删除数据库,或年轻教师因为压力大而点击了勒索邮件。因此,心理健康教育必须与网络安全教育深度绑定。辅导员和心理咨询中心要具备基本的网络风险识别能力,当发现学生有极端情绪或异常网络行为(如深夜大量上传下载数据)时,要及时干预。这种将心理疏导引入安全管理的做法,往往能在事故发生前切断导火索。最后,高校的管理者自身也要成为安全文化的践行者。如果校长的电脑用着盗版 Windows,如果教授的邮箱用着 123456 的密码,那么再多的教育都是苍白的。领导干部的数字素养提升,是构建校园安全文化的“第一块砖”。

总之,高校计算机网络安全教育管理,本质上是一场关于“人”的博弈。它不是单纯堆砌防火墙和杀毒软件,而是要通过课程的实战化改造,让学生“懂”安全;通过管理机制的融合,让部门“管”安全;通过校园文化的渗透,让师生“爱”安全。这 3 点并非孤立存在,而是互为支撑的螺旋上升结构。只有当安全意识内化为师生的本能反应,当安全管理从被动防御转向主动治理,高校的数字校园才能真正构建起一道坚不可摧的隐形防线。这是一项细水长流的工作,容不得半点形式主义,唯有务实、再务实,才能在日益复杂的网络空间中守住这一方育人的净土。

(杨斯淮/辽宁大学/讲师; 穆重怀/辽宁大学/教授)