CSTC中国评测 见证质量 技术白皮书

教育行业网络安全白皮书（2020 年）

中国软件评测中心·网络空间安全测评工程技术中心

2020 年 8 月

序 言

教育事业是民族振兴和社会进步的基石，教育行业信息化建设是提升教育发展质量，顺应历史发展趋势的必由之路。2010年以来我国大力开展教育信息化建设，2019 年政府报告中指出发展“互联网+教育”，目前我国教育行业信息化工程取得良好成效。2020 年初新冠疫情对传统教育模式带来冲击，在此影响下互联网在线教育再次发挥重要作用。云计算、大数据、物联网、移动互联网、虚拟现实等新技术在教育行业的应用不断深入，为教育事业的创新发展提供了新的技术支持，有效提升教育服务水平和教学管理成效。目前教育行业网络安全形势严峻，教育网络外部、内部环境普遍存在威胁隐患，同时存在数据安全、移动终端 App 等方面风险。

本白皮书内容聚焦教育行业网络安全的政策法规、发展现状、安全风险点，提出了加强教育行业网络安全防护的建议。

本白皮书的撰写人员有李世斌、李松恬、宁黄江、白利芳、张德馨、朱信铭、王涛、黄峥，在此特别感谢中国电子信息产业发展研究院副院长黄子河、副总工程师安晖、中国软件评测中心总工程师陈渌萍对白皮书的撰写指导，中心品牌推广部刘喜喜、闫晓丽的编辑及排版支持。

限于研究时间和编者能力，部分报告内容难免存在纰漏，不足之处恳请业界同仁批评指正。

中国软件评测中心 唐刚

2020 年 9 月 10 日

版权声明

编写指导：黄子河　安　晖　陈渌萍　唐　刚
编写小组：李世斌　李柁恬　宁黄江　白利芳
张德馨　朱信铭　王　涛　黄　峥

目　录

前　言

百年大计，教育为本。教育行业是我国最大的民生行业之一，教育事业发展是国家兴旺的不竭动力，推进教育行业信息化建设具备重要意义。2018 年 4 月 13 日教育部印发《教育信息化 2.0 行动计划》，2019 年政府工作报告中提出发展“互联网+教育”。随着国家政策引导以及移动互联网、5G、大数据中心等技术应用，教育行业信息化工程及在线教育平台迅速发展起来，智慧校园、远程教育、网络云课堂等方式受到广大师生群体认可。

教育行业机构多、系统多、数据多、影响面广，伴随信息化发展，教育信息系统面临着网络攻击、数据/个人信息泄露、勒索病毒入侵等网络风险，因此全面推进传统教育、在线教育、教育 App 的网络安全保障工作，提升教育行业整体安全防护水平至关重要。

本白皮书聚焦我国教育行业网络安全问题，从机构、人员、系统、应用等切入点对网络安全总体形势进行了分析并针对性提出安全保障建议。首先,从国家、地方层面对教育信息化时代的网络安全政策要求进行简要阐述；其次，对当前教育行业的网络安全总体形势进行分析；然后，对教育行业网络安全存在的风险原因进行了研究；最后，提出教育行业网络安全防护能力提升的相关建议。

中国软件评测中心（工业和信息化部软件与集成电路促进中心），简称中国软件评测中心，是直属于工业和信息化部的一类科研事业单位。长期服务和支撑国家部委、地方政府以及电信和

互联网、教育、卫生、广电、交通、能源、银行、证券、保险、航空等各大行业，业务范围覆盖全国31个省、自治区、直辖市，业务网络覆盖全国500多个城市，构建了基于第三方服务的科技产业链。

网络空间安全测评工程技术中心是中国软件评测中心核心业务板块，致力于信息系统的网络安全防护和安全运行，支撑政府主管部门履行网络安全相关的社会管理和公共服务职能，主营信息安全风险评估、网络安全等级保护测评、关键信息基础设施保护评估、数据安全能力和合规性评估等网络信息安全相关业务。

一、教育行业网络安全发展环境

(一)我国稳步推进教育信息化事业发展

教育信息化工程在教育领域运用现代信息技术，促进教育改革与发展，具备数字化、网络化、智能化、多媒体化等技术特征，以及开放、共享、交互、协作等教学特点。自 1993 年美国提出建设“国家信息基础设施”（信息高速公路计划）以来，世界各国纷纷探索教育信息化发展路径，我国的教育信息化事业也取得长足进展。

2010 年 7 月，中共中央国务院印发《国家中长期教育改革和发展规划纲要（2010—2020 年）》，提出教育发展战略目标，研究教育信息化建设可持续发展策略。

2012 年 3 月，教育部印发《教育信息化十年发展规划（2011-2020 年）》，提出以教育信息化带动教育现代化，把教育信息化摆在支撑引领教育现代化的战略地位。

2016 年 6 月，教育部印发《教育信息化“十三五”规划》，提出在 2020 年基本形成具有国际先进水平、信息技术与教育融合创新发展的中国特色教育信息化发展路子。

2018 年 4 月，教育部印发《教育信息化 2.0 行动计划》，积极推进“互联网+教育”发展，加快教育现代化和教育强国建设。

2019 年 2 月，中共中央国务院印发《中国教育现代化 2035》，提出加快信息化时代教育变革，建设智能化校园。

2020 年以来，教育部已启动《教育信息化中长期发展规划

（2021-2035）》和《教育信息化“十四五”规划》编制工作。

新时代，党中央、国务院高度重视教育信息化事业发展。自2015 年起《国务院关于积极推进“互联网+”行动的指导意见》已提出探索新型教育服务供给方式，探索网络化教育新模式。习近平总书记指出，实施“互联网+教育”，促进基本公共服务均等化。李克强总理在 2019 年政府工作报告中指出，发展“互联网+教育”，促进优质资源共享，发展更加公平更有质量的教育。当前教育信息化已成为改变传统教育模式、深化教育改革的重要内容。

(二)国家规划出台教育信息化网络安全政策

没有信息化就没有现代化，没有网络安全就没有教育安全，在教育信息化工程稳步前进的同时，国家教育主管部门在《中华人民共和国网络安全法》的基本法规基础上陆续出台一系列信息化安全建设与管理的政策法规，不断夯实教育行业网络安全保障体系。

2017 年 4 月，教育部印发《教育行业网络安全综合治理行动方案》，指出教育行业仍存在网络安全责任不落实、管理不规范、安全隐患修复不及时、监测预警和应急响应能力不足、网络安全事件时有发生等问题。教育部针对性开展了网络安全综合治理行动，包括治理网站乱象、强化主体责任、全面监测网络安全威胁、检测应用软件安全风险、补齐等保短板、加快完成定级备案、有序推进测评整改、加强关键信息基础设施规范管理、健全网络安全事件应急响应机制等。

2018 年 4 月，教育部印发《教育信息化 2.0 行动计划》，指出要建立网络安全和信息化统筹协调的领导体制，完善网络安全监督考核机制，以《中华人民共和国网络安全法》等法律法规为纲，全面提高教育系统网络安全防护能力，全面落实网络安全等级保护制度，深入开展网络安全监测预警，做好关键信息基础设施保障，重点保障数据和信息安全，强化隐私保护。

在此基础上，教育部于 2018、2019、2020 年连续部署“教育信息化和网络安全工作要点”，将网络安全工作与教育信息化并列提出，重点关注网络安全保障工作。在《2020 年教育信息化和网络安全工作要点》中指出，要不断完善教育网络安全支撑体系，网络安全人才培养能力和质量全面提升，教育系统网络安全防护水平不断提高，组织开展教育系统关键信息基础设施认定和检查。

2019 年 11 月，国家互联网信息办公室、工业和信息化部、公安部、市场监管总局根据《关于开展 App 违法违规收集使用个人信息专项治理的公告》联合制定了《App 违法违规收集使用个人信息行为认定方法》，为 App 违法违规收集使用个人信息行为的认定提供了参考；2019 年 11 月，教育部办公厅印发《教育移动互联网应用程序备案管理办法》，该办法中作出了现有教育移动应用的备案工作计划。

国家对教育行业网络安全高度重视，无论是教育机构、基层教育机构信息化建设，还是当前发展火热的“互联网+教育”“教育大数据”“在线教育平台”，国家出台的基础性法律、指导性政策、规范性文件和标准无不强调做好教育行业的网络安全工作。

(三)各地贯彻落实教育信息化网络安全部署

自教育部印发《教育信息化 2.0 行动计划》以来，各省市纷纷作出行动部署，切实推进教育信息化进程中的网络安全保障工作。

2019 年 3 月，黑龙江省教育厅印发《省教育厅关于进一步加强全省教育系统 招生考试网络与信息安全工作的意见》，指出要建立健全网络与信息安全工作组织体系、管理规章和责任制度；落实国家信息安全等级保护制度；有效防范、控制和抵御信息安全风险；增强安全预警、应急处置和灾难恢复能力；形成与教育信息化发展相适应的、完备的网络与信息安全保障体系。

2019 年 6 月，江苏省教育厅印发《江苏教育信息化 2.0 行动计划》，指出要推进“互联网+教育”大平台建设，探索互联网+教育服务模式。在云计算、大数据、物联网、人工智能等新一代信息技术深度融入教育全过程中，对教育信息化网络安全提出新要求。一是健全完善网络安全制度体系，要建立健全网络安全应急响应机制和应急预案，建立健全网络安全监测预警和通报制度，全面落实网络安全等级保护制度。二是健全完善网络安全技术防护体系，要配备软硬件设备设施和专业化队伍，建立技防与人防相结合的综合防护体系，构建可信、可控、可查的网络环境，有效防范和抵御网络安全风险。

2019 年 8 月，山东省教育厅印发了《山东省教育信息化 2.0 行动计划（2019—2022）》，文件指出要探索 5G 技术在无线校园建设中的推广应用，推进 IPv6 规模部署和应用，使教育信息

化应用分批次向云迁移。

自 2020 年以来，河北、吉林、广西、重庆、四川、陕西等多地印发了 2020 年教育信息化与网络安全工作要点。综合来看，多个省份在推进教育信息化 2.0 行动计划过程中，严格贯彻教育部部署，从教育信息化网络安全的工作管理制度、安全应急保障体系、网络安全应急预案、落实网络安全等级保护制度、建立健全教育网络安全监测预警体系、加强对重点教育网站的监测、开展网络安全专项教育和培训等方面作出了部署。

二、教育行业网络安全总体形势

教育信息化网络系统已成为当前建设教育强国的重要载体，为管理部门、学校、教师、学生及家长的使用提供了巨大便利。教育行业信息化应用系统每天产生并长期保存大量数据，包括教育资源、科研成果、师生信息、教学素材、国家教学资助信息等，因此网络安全防护工作与数据保护治理工作至关重要。目前教育行业网络安全形势严峻，高校校园网络、培训机构业务系统受到常态化网络探测与攻击行为，并在开学、招聘、重大事件等时段会加剧，主要风险点包括网络安全隐患普遍、校园网风险众多、外部环境攻击严重、内部环境漏洞增多、教育 DDoS 攻击频发、信息泄露事件不断、App 风险突出等。

(一)网络安全隐患普遍

随着互联网、移动互联网技术与传统教育行业深度融合，教育行业网络环境普遍存在安全隐患。教育行业信息系统具备网络、数据、用户规模庞大的特征，使得网络安全隐患分布广泛且监管防护难度增大。一是教育行业涉及人员众多，全国范围内教育机构有近 59 万个，专职教师 1800 万人，整体教育行业各级各类学生超过 3.5 亿人；二是教育信息系统数量多，教育系统网站超过 20 万个，edu.cn 域名的网站有近 11 万个，涉及超过 100 万人数据的系统达 500 多个；三是教育信息数据量大，教育行业政务数据资源数量达 10624 条，教师数据超过 4000 万条，累计学生数据超过 5 亿条。因此，教育行业信息系统特点可以总结为信息系

统多、业务类型宽、用户规模大、遍布地域广、软件类型杂、数据信息量大、信息价值高、用户信息化知识水平参差不齐、网络安全意识不强、管理制度执行难等，所有特征都是教育行业网络安全隐患普遍的诱发因素。

(二)校园网络风险众多

高等院校的校园网络和企业网络存在一定差异，因此网络风险及攻击面表现形式也有所区别。

一是校园网的高带宽和大规模特性导致网络病毒、木马程度蔓延迅速。高校的校园网是普及宽带网络较早的基础设施，因此已经实现普遍的千兆/万兆宽带在园区主干互联。校园网的用户群体比较密集，局域网内部用户规模庞大，一般都是集中的教学区、学生住宿区、职工住宅区等，而高带宽和大用户量导致了网络病毒、木马程序蔓延迅速，对严重的网络隐患表现出高敏锐性。

二是信息化运维难度大，管理流程复杂，导致风险管控和责任界定较难。高校无法像企业一样向每个员工落实网络安全防护职责，学生针对私人电脑进行的所有操作（例如 U 盘混用、不明网页浏览、不安全链接访问、木马病毒邮件查收等）都存在个人设备感染病毒后影响整个网络的风险。校园中的设备购置和管理情况非常复杂，除学校机房、教学设备、实验机房设备等由学校统一管理之外，学生和教师群体的个人设备无法由学校统一管控。一般高校的在校学生都在几万人左右，学生使用的是自己购买的设备（笔记本电脑、移动终端等）并由自己维护，这直接导致校园网络具备非常广的受攻击面，学生和设备众多，大家网络

安全意识和防护水平各不相同，并且发生网络安全事件后安全责任难以分清。

三是学生群体网络活跃度高，导致校园终端设备成为病毒、木马等传播的来源。在开放环境下，高校学生乐衷于尝试网络新技术，因此会有更大概率面临新技术带来的安全威胁。尤其各大高校计算机、软件工程、网络安全等相关专业的学生会研究各类木马病毒，亲身实验各类攻击技术，用个人电脑模拟攻击目标或者攻击靶场进行攻防实验，处理不当则可能对整个校园的网络造成影响和破坏。部分学生受好奇心驱使或者因科研需求，主动开发一些高危代码、制造漏洞、编制木马程序等，因而网络风险较高。

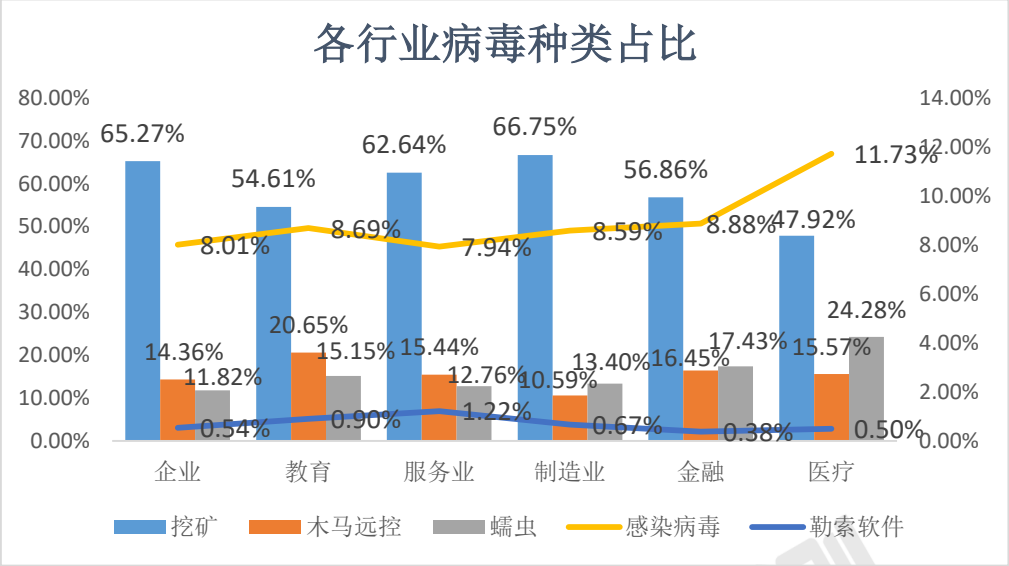
四是高校在网络安全防护方面投入有限，导致安全防护设备成为短板。高校是非营利事业单位，无法像商业公司一样大规模进行信息化建设与网络安全维护投入,因此高校存在一定程度的维护管理投入不足、网络安全技术手段不足、网络安全制度体系不足、网络安全意识淡薄等问题。

(三)外部环境攻击严重

信息系统外部环境威胁是指由系统安全区域边界之外引入的网络风险，如外部黑客等发起的拒绝服务攻击、端口扫描、木马后门、强力攻击、IP 碎片攻击、蠕虫病毒等。目前，教育行业网络面临严重的外部网络攻击，恶意软件表现非常活跃。深信服安全云脑检测到的 2019 年活跃的恶意程序拦截量为 181.07 亿次，其中挖矿类恶意软件感染占比最多（占 54.61%），其次为远程

控制木马（占 20.65%），蠕虫病毒也占有不小比例（占 15.15%）。

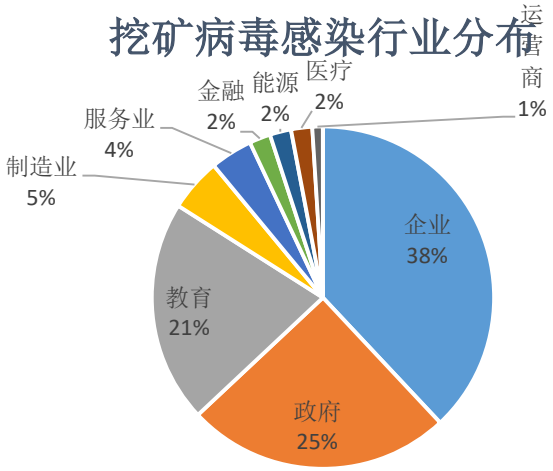
图 1：各行业病毒种类占比



数据来源：深信服千里目安全实验室

随着数字货币价值不断攀升，盗取用户计算机处理器的计算能力进行挖矿成为网络世界主要的威胁之一。从挖矿木马攻击的行业分布来看，黑客倾向于攻击企业、政府、教育行业。教育的拦截数量占拦截总量的 21%，占据第三位。

图 2：挖矿病毒感染行业分布



数据来源：2019 年上半年网络安全势态分析

(四)内部环境漏洞增多

信息系统内部环境威胁是指由系统安全区域边界以内引入的网络风险，如系统漏洞、网站脆弱性、管理制度缺失、安全运维能力不足等。目前，教育行业大量信息系统存在安全漏洞隐患。在《2017 年教育行业网络安全报告》中将教育行业细分为 8 个领域，每个领域抽样约 100 家机构，包括重点高校、职业培训、儿童早教、兴趣教育、出国留学、语言学习、教育信息化、综合服务&其他。对 800 家教育机构进行抽样分析，共发现 606 个 CVE 漏洞，19%的机构存在比较严重的安全漏洞，漏洞类型 Top5 为 OpenSSL FREAK Attack 漏洞、Microsoft Windows HTTP.sys 远程执行代码漏洞、IIS 6 远程代码执行漏洞、OpenSSL Heartbleed 心脏滴血漏洞、Ticketbleed 漏洞。该报告表示 93%的重点高校存在安全漏洞。从信息系统生命周期来看，从设计、编码到上线运行各环节都有可能造成安全漏洞，机构应建立完善的漏洞管理体系，加强人员管理、规范安全制度等全方位提升安全能力。

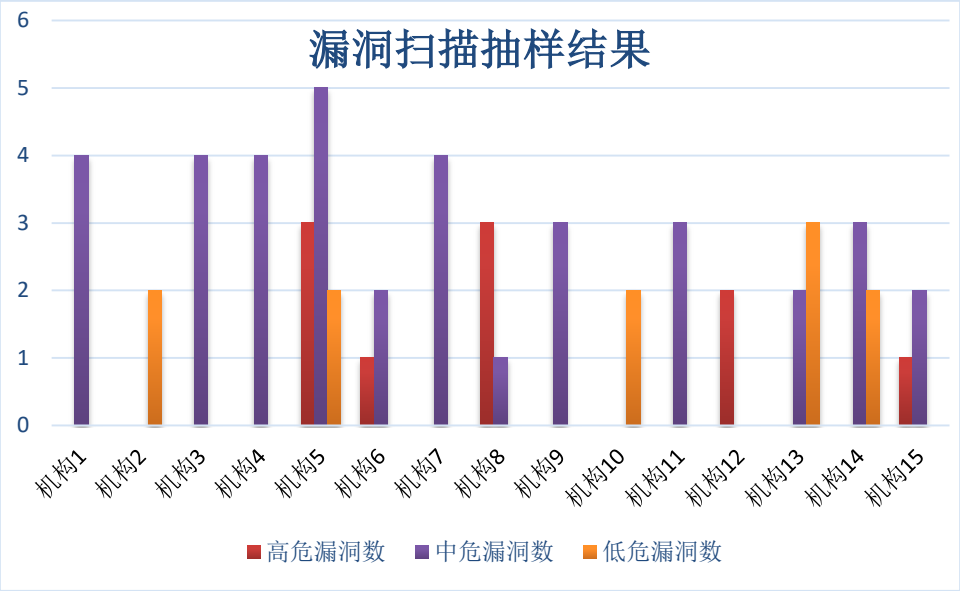
表 1：教育行业漏洞占比

领域	评估机构数量	漏洞机构占比	漏洞数量
重点学校	100	93%	497
职业培训	100	9%	11
儿童早教	100	8%	15
兴趣教育	100	4%	4
出国留学	100	8%	22
语言学习	100	9%	14
教育信息化	100	15%	32
综合服务&其他	100	8%	11
总体	800	19%	606

数据来源：2017 年教育行业网络安全报告

中国软件评测中心网络空间安全测评工程技术中心对具有代表性的一些教育行业机构进行抽样，分析可知抽样系统中主要以中危漏洞为主，部分系统存在 1-3 个高危漏洞。如果采用不同漏洞扫描器或者进行内部渗透测试，将可能发现更多漏洞，因此，教育行业网络安全形势严峻，内部环境漏洞依然众多。

图 3：漏洞扫描抽样结果



数据来源：中国评测网安中心

(五)教育 DDoS 攻击频发

拒绝服务攻击（DDoS）已经是当前互联网安全比较常见的威胁，DDoS 的危害在于无限制的消耗系统和网络资源，使其无法为正常用户提供服务。教育行业对系统安全可靠性要求高，需要长期稳定运行，因此 DDoS 攻击频发对教育行业影响较大。

根据 DDoS 攻击发生领域来看，不同领域受到 DDoS 攻击占比不同，其中重点高校占比最高。《2017 年教育行业网络安全报告》显示教育行业有 42%的机构受到 DDoS 攻击的威胁，其中重点高校最为严重，85%都遭受到不同程度的 DDoS 网络攻击，

47%的职业培训和44%的教育信息化机构遭受过DDoS网络攻击。

表 2：教育行业被攻击占比

领域	评估机构数量	被攻击机构占比	攻击事件数量
重点学校	100	85%	3402
职业培训	100	47%	21,080
儿童早教	100	31%	22,368
兴趣教育	100	34%	32,863
出国留学	100	33%	14,918
语言学习	100	38%	26,231
教育信息化	100	44%	22,583
综合服务&其他	100	27%	22,552
总体	80	42%	166,997

数据来源：2017 年教育行业网络安全报告

DDoS 攻击是一种常见的攻击方式，但在一些重大活动时DDoS 攻击会出现陡增态势。在一些重大活动时，如果 DDoS 攻击引起网络中断或部分业务不可用，则攻击造成的损失较为严重，这样的重大活动包括但不限于招生、迎新、重要领导视察、国家重大活动等，以及 2020 年的新冠疫情。2020 年的新型冠状病毒疫情对国内、国际的正常社会活动产生重大影响，教育领域也是受影响最严重的领域之一，全国科研机构、高等学府、大中专院校、小初高学校、各类培训机构都将教学、科研、管理等业务迁移到互联网线上进行。网络罪犯、黑客等不法分子注意到在线资源需求的增长，对最重要的教育信息系统及数字服务进行了攻击。据统计，2020 年 1 月 1 日至 3 月 22 日期间，全国教育行业在线网站/系统累计遭受 9600 多万次网络攻击。据阿里云安全运营中心监测，2020 年 1-3 月份抗击疫情期间应用层 DDoS 攻击量持续

处于高位，其中在线教育领域攻击量环比增幅靠前。

(六)信息泄露事件高发

教育行业的信息泄露威胁形势严峻。一是信息泄露事件频发。近年来教育行业信息各类泄露事件对师生人员和社会造成较严重负面影响，如学生个人信息泄露导致的经济诈骗事件、高校数据库泄露电子邮件元数据导致的重要信息泄露事件、新冠疫情期间海量学生个人信息泄露导致的网络骚扰辱骂事件等。二是教育网络运营机构和平台技术、管理环节的漏洞较多。教育行业缺乏针对海量数据进行统一处理的大数据平台，缺乏数据挖掘、分析、使用过程中的安全考虑，在信息系统建设、运行以及维护过程中，针对大数据的保护较为薄弱。此外，教育类 App 的个人信息保护仍存在不明地带，亟需建立覆盖个人信息采集、收集、储存、传输、使用、销毁等全生命周期的数据保障机制。三是教育行业师生群体个人信息保护力度不够、意识欠缺。高校的网络用户群体主要为广大师生，其受教育程度高，对信息化比较了解，上网率接近 100%，然而存在的问题是，高校用户规模庞大但网络安全意识不强，安全素养和技能参差不齐，使得网络数据安全问题突出，信息泄露事件不断，这成为高校信息化中安全管理的一大难题。

(七)App 网络风险突出

教育类 App 的网络安全问题主要表现在技术能力不足、管理制度不完善、权限采集不合规、数据安全问题突出等几个方面。

一是部分 App 技术能力不足和管理制度不完善。自“互联网+教育”理念推出及相关政策出台以来，市场上涌现出大量教育 App。然而部分 App 从教学模式构建到产品研发运营的周期较短，前期准备不充分，网络安全技术防护措施及安全管理制度相对不成熟。

二是部分 App 存在违规采集用户数据、过度获取移动终端系统权限的问题。这类 App 声明权限超出业务实际使用范围（如某教育 App 在权限声明中提到了读取通讯录、编辑通讯录及访问精准定位等权限，但实际上软件并不含有与此权限相关的功能）；与此同时，App 收集个人信息行为不规范，在用户关闭电话权限的情况下仍然会收集用户的部分设备信息、IP 地址等。2020 年 6 月 8 日央视一套《朝闻天下》报道，某教学 App 后台偷窥用户隐私，在十几分钟时间里访问手机照片文件近 25000 次。而教育行业类似的流氓 App 还有许多，在没有登录、没有授权、并非在学习和上课状态下，仍然自由访问读取手机信息，获取手机内用户通讯录、短信、照片库等隐私信息。

三是 App 的数据安全、内容安全问题突出。除了技术层面的数据泄露风险外，App 内容安全问题也成为突出问题，亟待解决。教育类 App 在用户量激增情况下为了最大化追求商业利益，会采取植入广告、推荐网络游戏、过度娱乐化、涉黄涉赌信息传播等问题。据北京阳光消费大数据研究院统计数据显示，2020 年 1 月 1 日至 5 月 26 日，共监测到有关网课、网游和网络打赏等舆情信息 2072233 条。其中，网课舆情信息 1043735 条，占比 50.37%；网游舆情信息 791746 条，占比 38.21%；网络打赏舆情信息 236752 条，占比 11.42%。可以看到移动互联网技术拉动视频直播等行业兴起，而在线教育融合网络直播后，其内容安全成为隐患，教育行业用户群体在面对直播平台、在线网课中植入的大量游戏、旅游、色情、暴力等诱惑时难免不会有

人中招。事实上，在 2020 年上半年已经发生多起教育类平台充斥网游广告，未成年学生参与网络付费游戏与网络直播平台“打赏”的事件。

三、教育行业网络安全问题分析

教育行业网络安全形势严峻，因为网络攻击面广泛、校园网用户群体安全防护能力不一、内外部威胁升级、教育 DDoS 频发以及信息泄露风险增强等因素，导致教育行业应用、数据面临的主要威胁现已发展到了新的阶段。中国软件评测中心网络空间安全测评工程技术中心对教育行业重要信息系统进行检查、等级保护测评、网络安全风险评估、以及漏洞监测挖掘，总结出教育行业仍存在的主要安全问题，首先是对教育信息系统的网络安全重视与投入不足，等级保护工作落实情况不佳；其次，教育信息泄露风险难以管控，网络安全管理不到位；此外，在线教育平台安全防护力度不够，防护能力薄弱。

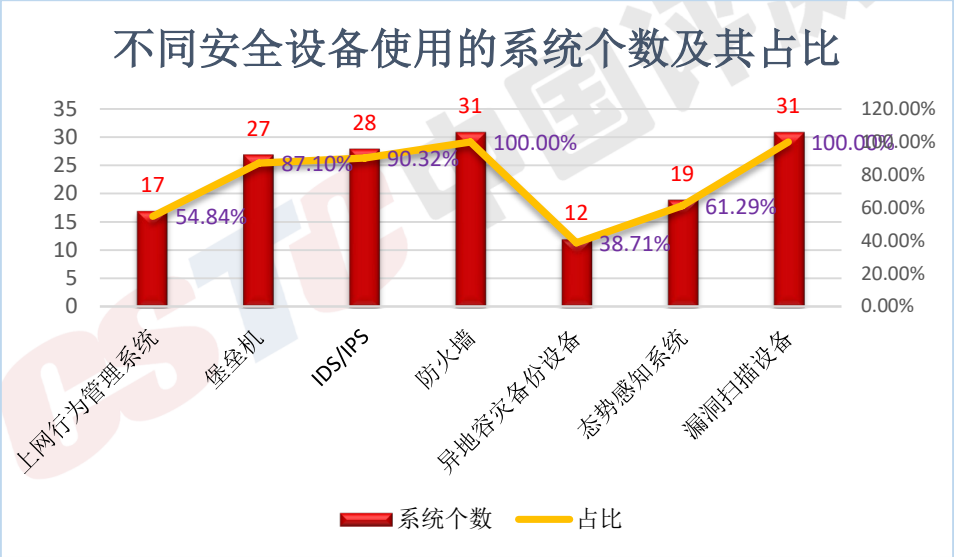
(一)网络安全重视力度不足

从全国总体来看，当前教育行业的网络安全投入普遍偏低，管理不善，存在未定期进行信息系统网络安全测评、网络安全设备应用率低、未定期进行漏洞扫描等问题。

中国软件评测中心网络空间安全测评工程技术中心结合对教育行业高等院校、培训机构、教育平台和 App 的网络安全评估数据，针对 2019 年具有典型性、代表性的一些教育机构（以下简称样本机构）的测评数据进行了抽样分析，大部分样本机构

主要依靠防火墙设备和漏洞扫描设备作为基本的安全防护设备，防火墙设备和漏洞扫描设备应用率为 100%，IDS/IPS 使用率为 90.32%，堡垒机使用率为 87.10%。分析数据可知样本机构不同程度进行了网络安全测评并上线了安全设备，但仍然存在安全问题，除了防火墙等常规安全设备外，态势感知系统、上网行为管理系统、异地容灾备份设备的应用率分别为 61.29%、54.84%、38.71%，安全网闸、防病毒网关、安全审计系统等设备也未见上线应用，样本机构在信息系统建设过程中，对网络安全的软硬件投入不足，新型网络安全设备应用率较低，防护类型单一。

图 4：不同安全设备使用的系统格式及其占比



数据来源：中国评测网安中心

调研数据显示，样本机构中仅 29%的机构在信息系统建设与上线过程中进行了第三方网络安全验收测试。同时，聘任了专业的网络安全人员作为安全顾问的机构占比也只有 29%。通过调研管理制度发现教育行业人员对网络安全重视力度不够，存在“得过且过，形式上通过”的现象。

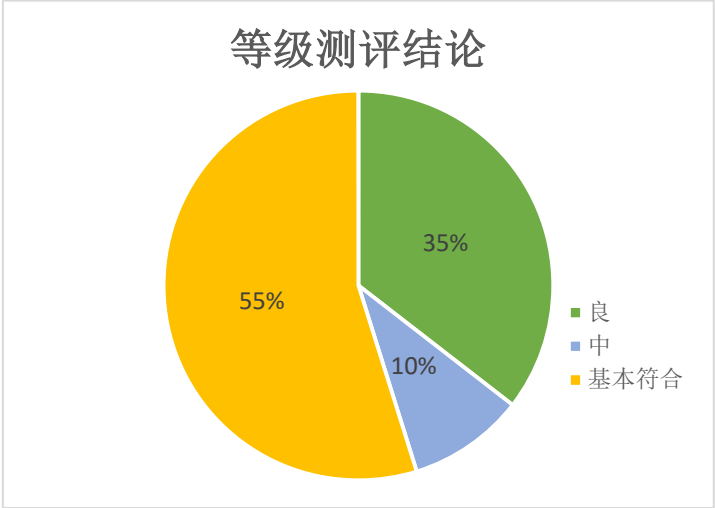
(二)等级保护落实情况不佳

自 2017 年《中华人民共和国网络安全法》颁布以来，网络安全正式进入法制时代，履行网络安全等级保护制度成为了网络运营者的基本义务。然而目前教育行业的等级保护制度落实情况还需进一步推进。迄今为止还有一定数量的高校、培训机构、在线教育平台未做过等级保护测评，而做过等级保护测评的机构中有相当比例存在一些测评项不达标、存在中危漏洞、测评分数不够高等情况。教育行业亟需加快落实步伐，进一步梳理信息系统，开展等级保护测评和系统安全加固工作。

中国软件评测中心网络空间安全测评工程技术中心结合对教育行业高等院校、培训机构、教育平台和 App 的网络安全评估数据，针对 2019 年具有典型性、代表性的一些教育机构等级保护测评数据进行了分析。样本采集空间覆盖了多个教育领域从业机构，包括重点高校、普通职业院校、小初高学校、培训机构、在线教育平台等，样本采集时间覆盖了 2019 年等级保护 2.0 实施之前到等级保护 2.0 标准正式实施之后。

针对被抽样的样本数据进行整理分析，进行网络安全等级保护测评后只有 35%的机构的信息系统达到良，55%的机构的信息系统测评结果为基本符合，而其余 10%测评结果为中等。

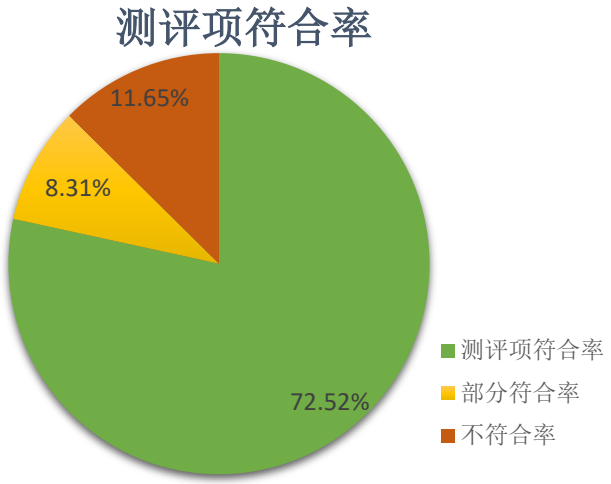
图 5：等级测评结论



数据来源：中国评测网安中心

从技术层面、管理层面的测评项符合率分析，符合率平均值为 72.52%，部分符合率平均值为 8.35%，而测评项的不符合率超过了 10%，平均值达到了 11.65%，说明被抽样教育机构在落实等级保护制度过程中，仍然有部分指标项不符合。

图 6：测评项符合率



数据来源：中国评测网安中心

针对测评结果的问题项进行分析，被抽样机构信息系统中，平均每家机构的问题总数在整改后达到约 38 个，其中高风险级别的问题 0 个，中风险级别的问题整改后还有约 29 个，低风险

级别的问题整改后约 9 个。在信息系统初测时问题项更多，经过运营方、开发方、测评方对重要问题提出整改方案，整改后仍然存在约 38 个问题项，因此信息系统的等级保护安全防护工作仍需加强。

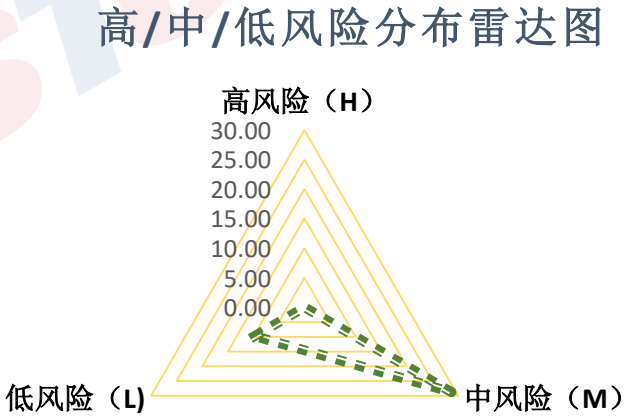
表 3：测评项符合率占比及剩余风险问题个数

综合得分	测评项符合率	部分符合率	不符合率	问题数总计	高风险（H）	中风险（M）	低风险（L)
83.96	72.52%	8.35%	11.65%	38.45	0.00	28.72	9.72

数据来源：中国评测网安中心

针对以上高、中、低级别的风险通过雷达图进行综合分析可知，信息系统主要脆弱性的风险级别被判定为中风险级别，其问题量占比较高，由此可以预测教育领域其他信息系统的风险评估结果中，大部分将集中在中风险区间。

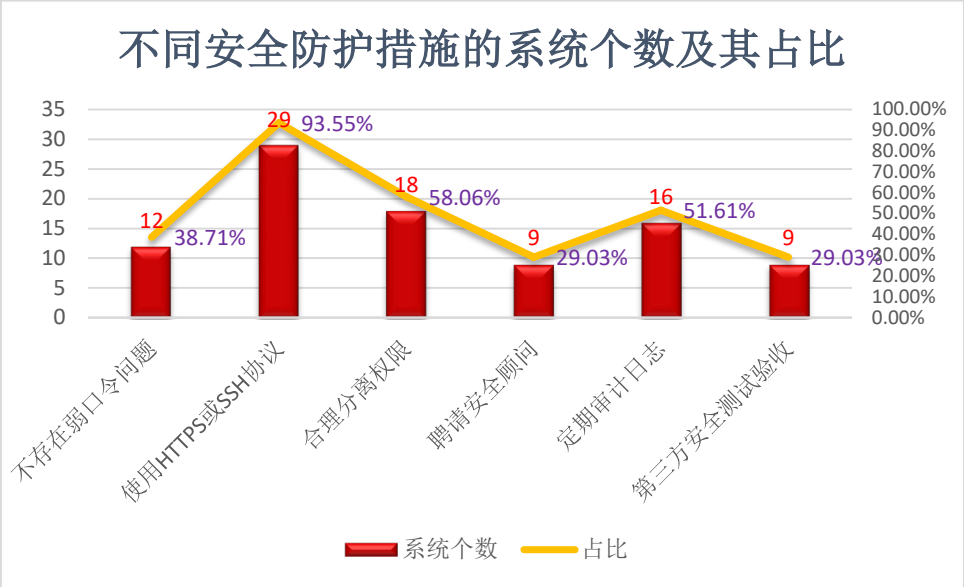
图 7：高/中/低风险分布雷达图



数据来源：中国评测网安中心

对被抽样的信息系统测评结果中具体的安全防护措施落实情况进行分析，从下图可以看出技术方面和管理方面的安全防护措施仍然不足。

图 8：不同安全防护措施的系统个数及其占比



数据来源：中国评测网安中心

一是存在弱口令问题。样本机构中不存在弱口令问题的系统占比只有 38.71%，这一比例明显偏低，意味着还有近 62%的系统存在弱口令隐患；当前各大高校信息系统大多采用安全性较弱的“学生学号+口令”的单认证方式，鲜有采用“双因素认证”等强认证方案，高校信息系统的信息安全程度与登录口令的强度直接相关。信息系统用户多采用易被别人猜测到或易被工具破解的弱口令，使得攻击者甚至无需技术基础就可对目标系统进行攻击。一旦口令被破解，攻击者即可对目标系统进行进一步渗透。在安全测试过程中主要发现简单口令、默认口令或空口令、规律性口令、社会工程学弱点类口令等情况。

二是合理进行权限划分的机构占比偏低。样本机构中进行合理的权限划分的只有 58.06%，因此教育信息系统运营机构应进一步配备网络安全管理人员，使系统管理员、安全管理员、审计员等账号权限分离。

三是定期审计日志的占比 51.61%，将近一半的被测信息系

统未定期审计系统安全日志，在信息安全事件应急响应与原因追溯方面尚需发力。

四是聘请安全顾问与第三方机构进行安全验证测试的占比只有 29.03%，表明机构在执行等级保护制度时并未严格按照等保标准、安全相关法规制度进行系统安全防护。

(三)安全风险管控手段落后

近年来，国内外教育行业已经发生多起数据库泄露事件，相关人员隐私权益遭受严重损害，涉案企业、机构声誉大打折扣，教育行业信息泄露原因多样导致风险难以管控。

一是相关标准规范制定滞后。随着教育信息化的快速发展，教育机构、在线教育平台等掌握的隐私信息爆发式增加，在个人数据保护、教育信息防泄露等方面的标准规范和测评规范需要及时跟进。《中华人民共和国网络安全法》规定网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并获得同意；网络运营者不得泄露、篡改、毁损其收集的个人信息；任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或非法向他人提供个人信息，并规定了相应法律责任。GB/T 35273-2020《信息安全技术 个人信息安全规范》正式发布并规范了互联网信息化进程中的公民个人信息保护原则和要求。作为推荐性国家标准，其只是在企业的网络安全合规建设、信息保护与权限采集过程中起到参考作用。2020 年 5 月 25 日，十三届全国人大三次会议上全国人大委员会工作报告中指出将制定个人信息保护法、数据安全法。其实 2019 年 12 月实施的等保 2.0 标

准已经把大数据安全纳入监管体系，2019 年 5 月国家互联网信息办公室发布的《数据安全管理办法(征求意见稿)》也在个人隐私、App 过度索取权限等涉及隐私泄露等问题方面做出了明确规定。2020 年 5 月 28 日通过的《中华人民共和国民法典》第六章“隐私权与个人信息保护”明确了隐私权、个人信息的定义，以及个人信息主体的权利和信息处理者的安全和保密义务等内容。我国正在逐步建立个人数据保护相关的基础法律体系，因此需要同步制定适用于教育行业的细化法规、标准、规范体系。

二是管理措施不够完善。教育机构各类业务系统的快速增加，各类隐私信息分布存储在各个业务系统和办公终端上，导致业务分散且增加了管理难度，相应管理措施很难实时掌握敏感信息状态。

三是数据库防护手段薄弱。当前教育行业相关单位的主要安全防护手段以网络各区域实施访问控制策略为主，以防火墙、入侵防御相关设备策略为辅来实现访问控制与数据保护。但针对数据库本身漏洞的防御能力低，数据库产品暴露 0-day 漏洞、受 SQL 注入攻击等情况可能成为安全短板，给黑客可乘之机。

四是大量数据以明文形式存储。随着教育行业信息化程度的提高，学籍、身份、健康、成绩等大量敏感信息集中存储在数据库系统中。数据明文存储机制使得敏感数据面临被篡改、被窃取的威胁，安全风险大大增加。

五是监控手段不足。敏感、隐私信息在教育机构各类业务系统中相互频繁调用，没有有效的监控手段，导致非法调用、越权使用、违规批量下载等行为严重失控，如果教育机构在数据管理

过程中不进行主动脱敏，则敏感信息泄露的风险进一步增加。

(四)网络安全管理监督缺位

当前教育行业存在不同程度的网络安全管理制度不完善、机构安全管理职责不明确、人员网络安全意识薄弱、事前和事中监督缺位严重等问题。

网络安全管理制度包括信息安全管理总体方针策略、安全管理活动制度规范、日常管理操作规程表单等，是信息系统的建设、开发、运维、升级和改造等环节遵守的行为规范总体。未制定网络安全管理制度或信息安全管理制度不完善，将无法对信息安全管理过程中的行为进行规范和约束，增加了由于人员操作失误造成信息安全事故的风险。同时，教育机构如无完整的网络安全事件应急响应预案，或者未形成应急演练机制，则应对重大安全事件的能力和业务恢复能力都无法得到验证。

网络安全管理机构职责不明确将导致网络安全管理制度无法有效落实，无法使网络安全管理制度产生相应的效力，增加网络安全事件发生的风险，同时也是网络安全事件发生后管理职责不明、责任划分不清、风险溯源困难的原因。

网络安全管理人员安全意识薄弱是造成信息泄露事件、运维过程中产生重大失误、系统攻击面增加的重要原因。网络安全管理人员的安全意识和业务能力没有保障，则人为操作失误带来的风险的可能性增加。

事前和事中监督形同虚设，存在缺位现象，一旦遭遇网络安全事件，用“事后监督”来弥补，但是事后监督存在滞后性、被动

性，无法充分保证网络运营和教育数据资源流通的全流程安全。教育行业中态势感知系统、上网行为管理系统、第三方网络安全验收测试、专业网络安全顾问等安全防护与管理措施缺位，进一步导致对教育信息系统缺少刚性监督，无法保证安全管理机构、安全管理制度、安全管理人员等措施的实效。

(五)在线教育防护能力薄弱

在线教育平台的迅速崛起和发展对教育行业引入了新的网络安全风险，从侧面反映出在线教育平台的安全防护力度依然不够。

在线教育平台依托云计算资源是一种广泛采用的服务方式，云计算环境使得教育数据面临的安全威胁更为复杂。一是外部威胁层出不穷，云平台、租户都可能成为入侵对象且威胁类型多样（如拒绝服务攻击、端口扫描、木马后门、强力攻击、缓冲区溢出攻击、IP 碎片攻击、蠕虫病毒等）；二是云平台存在虚拟机滥用、租户隔离失效、数据被泄露、篡改或丢失、应用程序接口安全以及代码级安全等问题；三是在云服务模式下安全责任划分不清晰、业务权限不透明、难以进行数据审计追责等问题，云平台和租户要时刻保持“在线教育上云无法做到绝对安全”这种意识。

同时，在线教育平台和教育信息系统运营机构在数据安全管理方面存在盲区。在线教育平台通过账号注册采集、检索与审计、网络爬虫等技术可以获取学生基本信息、家庭信息、学习信息、恋爱社交信息及其他敏感数据。一些在线学习 App 推出课程订阅与资料采购服务，需要进行实名身份认证，个人基本信息、金

融支付信息、物流收货信息是必须采集项。目前没有源码审计、白盒审查之外的方法可以判别应用是否访问通讯录、聊天记录、个人浏览记录等信息，但毫无疑问这些都属于敏感个人信息。在线教育平台在进行用户数据提取与业务处理过程中存在着数据安全管理盲区。一是数据收集过程中存在过度问题；二是数据处理使用过程中未有效通过技术和管理并重的方式进行数据安全保护，例如一些招考平台在公布考生成绩时将身份证号、出生日期、手机号等一同公布；三是平台、师生用户的信息保护意识不强。

四、教育行业网络安全保障建议

根据纵深防御思想以及等级保护制度中一个中心、三重防护的理念，结合教育行业网络安全总体形势和在线教育平台及 App 安全保障需求，中国软件评测中心网络空间安全测评工程技术中心提出以下教育行业网络安全保障建议。

(一)切实做好基础设施安全防护

教育信息系统、在线教育平台运营者需重视网络基础设施的安全防护。物理安全是系统安全的基础，保障系统物理安全工作的重点是保护机房安全。如果机房环境遭到物理破坏或非法入侵，那么系统将直接不可使用或者发生数据泄露，这是对系统最简单直接彻底的破坏。这种安全威胁不需要任何技术手段，部署的安全产品都无法发挥作用，所以机房安全建设是最基础的防护措施。

无论是教育机构自建机房还是云平台托管机房，其安全运营维护需要关注以下几点。

■使用专用的物理空间建设机房。机房所在的建筑物应具有防风防雨防震能力，且不能在建筑物的顶层或地下室。

■确保机房附近没有水源，防止用水设备故障影响机房设备正常运行。

■为机房设置门禁系统并避免闲杂人员访问，控制、鉴别和记录进入的人员。

■做好防雷击、防静电、防火、防水和防潮措施，尤其是机柜、设施和设备进行安全接地并采用必要的接地防静电措施，采取措施防止感应雷，防止机房和空调系统的水蒸气结露和地下积水的转移与渗透。

■确保机房具备冗余供电措施，建设灾备机房并实时备份数据。

(二)持续推进三重防护安全建设

教育信息系统、在线教育平台运营者需严格按照“一个中心，三重防护”的安全建设理念，持续推进网络三重防护建设。网络三重防护包括安全通信网络、安全区域边界、安全计算环境，涵盖了交换机等网络设备、防火墙等安全设备、服务器等计算存储设备、操作系统与中间件等软件基础设施、数据库与业务系统等上层应用。

1. 建设安全通信网络

安全通信网络是系统网络架构的部署形式，设计合规的网络

架构是保证网络、通信传输、可信验证等安全要求达标并保护信息系统安全的前提。如果系统网络架构存在安全缺陷，则很难通过其他安全防护措施进行弥补，并且后期的整改费用昂贵。因此，从网络规划阶段就应重视网络架构安全设计，建议重点关注以下安全通信网络建设要点。

■ 安全划分子网。分出数据存储区、非军事区（DMZ 区）、运维区、办公区等子网，如有必要根据职能不同对办公区做进一步细分。不同子网间部署防火墙进行隔离，避免将重要网段部署在网络边界处，通信线路和关键设备要有硬件冗余。

■ 配置细粒度的访问控制策略。根据测评经验可知现在大部分系统的访问控制策略没有设置到协议端口，并且源 IP 地址和目的 IP 地址的范围偏大。建议根据业务理清 IP 间相互访问规则和其间的访问协议，并确保运维区不能直接访问互联网。

2. 建设安全区域边界

安全区域边界是系统实现边界防护、访问控制、安全审计、入侵防范和恶意代码防范、可信验证的重要基础，使用安全设备提高网络安全防护能力也是教育信息系统安全运行的必要措施。网络中应部署 IDS/IPS、防毒墙、WAF、资源监控系统、垃圾邮件检测系统、上网行为管理系统、堡垒机、日志服务器等安全设备，并定期更新安全设备的规则库和系统版本。通过部署堡垒机对系统设备提供统一登录管理，集中实现双因素认证、用户权限分配、安全审计功能是当前普遍采用的性价比较高的方法之一。

3. 建设安全计算环境

安全计算环境包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护等防护内容。基于教育行业网络安全风险点以及中国软件评测中心网络空间安全测评工程技术中心对样本机构的脆弱性分析，建议重点关注登录口令复杂度、账户权限分离、安全审计等内容。

设备和软件安全的第一道防线是身份鉴别，黑客攻击系统的一般方法首先是猜测或爆破登录口令然后再进行其他破坏操作，建议从以下几方面加强用户口令安全。

■ 严格按照网络安全等级保护标准要求，为设备和软件配置符合标准规范的口令并定期更新。

■ 避免存在设备出厂默认口令。教育行业绝大部分机构具备公立事业单位属性，信息系统及应用都由机构的信息中心自主运维，但是设备采购类型存在交叉重叠，针对大量同一供应商的产品广泛应用到教育机构的情况，应强制运营人员修改网络设备、安全设备、计算设备、存储设备的出厂默认口令（如 admin、cisco、huawei 等出厂默认口令在业内类似于明文存在）。

■ 避免使用共享账号，严格落实账号权限分离策略。高校信息中心等部门应进行职权划分，不同角色的管理员使用不同运维账号，避免使用同一个账号登录系统。针对在线教育平台等使用了云平台或者托管机房的机构，应明确责权、实现计算资源

的逻辑隔离与物理隔离，合理分配自主运维账号、厂商运维账号的权限。

■ 使用双因素身份鉴别方式。双因素认证的两种身份鉴别方式建议为系统用户所知、用户所有，并保证用户所有的口令设备基于密码技术（如 Ukey、动态令牌等）。

安全审计功能目的在于进行网络安全事件溯源、安全事件处理、系统故障修复、运维记录审计、事件预防与事后惩戒等。一旦发生安全事件，完备的审计记录是攻击源追溯与系统修复的重要途径。建议关注以下几个方面。

■ 对重要用户行为进行审计。关注用户登录退出、修改口令、修改用户权限等事件的审计。

■ 保护审计进程。防止审计进程受到未预期的中断。

■ 实时备份审计日志到日志服务器。攻击者攻击系统后会清理攻击痕迹，所以要保护审计进程和审计记录。使用网络审计和数据库审计系统对日常操作行为进行审计。

(三)重点提升信息泄露防护能力

教育信息系统、在线教育平台运营者需从技术、管理层面同时发力提升信息泄露防护能力。师生群体以及其他线上教育参与者需要增强数据安全保护思想意识。

1. 提升数据安全保护技术能力

运营重要信息系统，掌握大量教育数据的机构（如教育主管部门、重点高校、教育领域协会组织、国家教育基础设施与电子资源库、其他教育数据中心等）可提升以数据安全为核心的防护

技术能力，来保证教育信息安全，避免数据泄露事件频发。一是针对运营的海量教育数据建立一个统一的大数据处理平台，对产生的数据进行保护、挖掘、分析以及利用，对数据特征进行识别；二是通过高强度、安全可靠的透明加密为重要信息提供有力保护，保证敏感关键信息无论何时何地都是加密状态，可信环境内，加密文档可正常使用，在非授信环境内则无法访问加密文档；三是建立全面的信息防泄露溯源追责机制，通过防泄露技术进行技术防护，通过完整的文档、操作审计发现风险触发点，做到事中研判防御，事后溯源追责。

同时，广泛调研国内大数据关键技术发展情况，实现教育领域大数据安全技术可控是保护数据安全的重要手段之一。在教育行业信息系统的建设、运营、大数据中心搭建、教育机构门户运维等工程中支持国内研发的产品应用，为大数据关键技术发展提供更稳定安全的环境。

2. 健全数据安全保护制度体系

针对教育行业个人信息保护工作不佳，数据泄露事件时有发生的情况，应当从立法、立标、树规、贯标等方面对信息安全技术防护体系进行管理上的补充，提升“三分靠技术，七分靠管理”的安全意识。

目前数据安全与个人信息保护相关法规正在研制出台中，数据安全合规性需求将进一步加大，针对数据安全保护、信息泄露事件的监管将进入法制时代，基础法规的颁布需要行业领域内制定具体的标准规范进行贯彻，通过国家标准或者行业标准来对教

育行业关键信息、敏感数据进行分类分级管理。可以用数据标签对创建数据、应用数据、存储数据、传输数据和销毁数据提供技术上和操作上的规范要求。对于关系到教育行业发展以及系统用户个人信息的重要数据，需严格控制其存储位置、传输和使用方式。

3. 增强数据安全保护思想意识

在教育行业中的数据泄露问题处理方面，尤其需要增强用户的网络信息安全意识。针对受教育群体而言，他们是教育信息系统、在线教育平台、App、微服务等应用程序的前端用户，需要提升应用使用安全意识，形成安全习惯。一是开启个人电脑的防火墙，安装木马和病毒查杀软件，养成定期进行 PC 端、移动端病毒查杀与漏洞扫描的习惯；二是更换手机时及时删除个人信息，注销使用过的教育平台账号时需要将历史记录，敏感信息进行清除；三是谨慎使用公共 WIFI，尤其是一些无密免费 WIFI；四是不轻易填写在线调查问卷，例如关于个人学习规划、出国深造计划、个人学习环境、家庭教育理念等调查时往往要求填写详细的个人信息；五是与同学和亲友等熟人交往时保持一定程度的警惕，因为黑客会充分利用社会工程学攻击手段，通过好友身份逐步接近被攻击者，通过亲友信任感逐步欺瞒获取口令与权限，因此要严格遵循敏感信息最少化、密钥信息不泄露的原则，谨防社会工程学攻击。

(四)全面建设安全管理监督体系

1. 建立应急响应预案机制

教育机构如无完整的网络安全事件应急响应机制，则应对突发安全事件的能力无法保障。因此，要严格落实《中华人民共和国网络安全法》要求，重视并建立教育系统网络安全应急预案，进行预案培训与演练，在教育领域内高校、培训机构、在线教育平台等机构根据自身组织特点差异及时修订并优化应急响应预案，形成网络安全应急保障协调联动机制，提升应急处置能力，保证发生安全事件时系统运维人员能有步骤有策略地应对，降低机构和社会损失。

2. 完善信息安全管理体系

针对网络安全管理制度不完善、机构安全管理职责不明确、人员网络安全意识薄弱等问题，针对性地制定机构内部制度体系，使安全管理工作步入常态化、规范化。教育行业的主体是重点高校、普通职业院校、小初高学校、培训机构、在线教育平台等，对于科研高校等非市场化经营的机构而言，在没有进行 ISO 27001 信息安全管理体系认证的情况下，要对已有信息安全管理体系进行整改完善，一是建设符合 ISO 27001 标准的信息安全管理体系，包括总体方针策略、各类网络安全活动制度、日常管理操作规程、制度落实的记录表单等；二是教育机构结合自身教学业务特色，充分借鉴 ISO 27001 标准中 PDCA 循环的思想，在人、技术、操作三层面建立可持续优化的安全防护体系。

3. 加强网络安全人员管理

网络安全管理人员安全意识薄弱是造成信息泄露、运维过程中产生重大失误、系统攻击面增加的重要原因。因此，要建立内部运维管理团队，提高人员网络安全专业技能和网络安全防护意识。教育行业信息化进程中对网络安全人才不可或缺，而现在教育体系里不但缺少网络安全人才，而且缺少计算机专业人才，不能专业地完成信息化建设工作。服务外包形式的前提要有自己的专业人员领导，能够把控外包给第三方公司所存在的安全风险。一是完善岗位设置，在人力资源充足的条件下尽量避免网络管理员、安全管理员、安全审计员这三个岗位兼任。二是加强人员培训，根据业务需求为不同人员提供与其岗位对应的技能培训。不但要进行技术人员培训，系统使用者的培训也尤为重要。三是强化人员考核，通过考核督促相关人员主动提高专业技能，并提高培训效果。

(五)全面开展在线教育系统等保测评

一是通过等保备案、测评工作，规范在线教育平台建设，提升安全防护能力。在线教育平台及教育行业大数据平台运营方（学校、培训机构、云厂商）应该按照《中华人民共和国网络安全法》、《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的规定，严格落实国家网络安全基本要求，教育领域信息系统作为关键信息基础设施，需严格按网络安全等级保护制度进行保护。网络安全测评机构作为大数据安全保障的主力军，需要对教育大数据平台运营者进行全流程的安全咨询、测试、评

估、认证、培训。测评机构除了提供基于等级保护的基础测评服务外，还应保持对数据与风险的敏感性，持续提供网络安全态势感知、高级持续威胁（APT）检测、大数据平台渗透、漏洞挖掘等专业增值服务。

二是通过开展等保备案、测评工作，做好在线教育平台个人信息保护工作。在线教育平台和应用开发方应在技术层面深入分析大数据平台基于开源软件、按需搭建的架构，对于此类情况的应用应重点进行安全防护，并进行网络安全风险评估，大数据平台应用、接口、App 应进行源代码安全审查与渗透测试，查补漏洞防止发生信息泄露事件；在管理层面要提升数据治理能力，做好多源数据汇集与敏感数据脱敏等工作，防止在数据开放、共享过程中存在泄露、滥用等安全问题。

(六)引导规范教育 App 合规性备案

教育 App、在线教育平台运营者需严格进行 App 合规性备案，行业监管机构和安全服务商应引导教育机构完成教育 App 合规性备案工作。

2019 年 8 月，教育部、中央网信办、工业和信息化部、公安部等八部门联合印发《关于引导规范教育移动互联网应用有序健康发展的意见》，将教育 App 进行分类。2019 年 11 月，教育部办公厅印发了《教育移动互联网应用程序备案管理办法》，该办法高度重视教育移动应用备案工作，要求分阶段完成教育移动应用备案工作，并将 2019 年 12 月 1 日至 2020 年 1 月 31 日列为 ICP 备案和等级保护备案缓冲期。教育移动应用提供者未在 1 月

31 日前完成 ICP 备案和等级保护备案的，其教育移动应用备案将被撤销并予以通报。截止 2020 年 4 月底，教育移动互联网应用程序备案管理系统累计公布了 1431 家企业的 3180 个教育 App 备案。2020 年 5 月，教育部科技司发布了《关于做好教育 App 的 ICP 备案和信息系统网络安全等级保护定级备案工作的公告》，公告表示教育 App 的 ICP 备案和信息系统网络安全等级保护定级备案时间因新冠疫情影响而延期至 2020 年 6 月 30 日。7 月 1 日起，将对未按时完成备案的教育 App 提供者进行通报，并限时 1 个月整改。对于 7 月 31 日前未完成整改的，将撤销其教育 App 备案。同时，ICP 备案以工信部网站查询截图为准，网络安全等级保护定级备案以公安机关的备案证明为准。

教育、互联网电信主管部门高度关注教育移动互联网应用程序 App 备案工作。教育 App 应用程序量大、用户规模众多、处理数据广泛，因此提升行业整体网络安全防护能力的必要条件是补齐木桶原理中的每一环节短板，后续需要监管机构和 App 开发运营机构共同发力，引导规范教育移动互联网应用程序 App 的合规性备案工作，同时进行 App 应用符合性评估，充分保证 App 安全。

五、教育行业网络安全的等级保护 2.0 推进

从 2019 年开始等级保护制度进入“等保 2.0”阶段，同时有相关的“等保 2.0”标准出台，包括 GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》、GB/T 28449-2018《信息安全技术 网络安全等级保护测评过程指南》、GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》、GB/T 25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》、GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》等，这些标准对于等保定级、备案、设计、测评、整改等过程有了新的要求。“等保 2.0”标准在“等保 1.0”标准的基础上增加了云计算、大数据、物联网、移动互联网的安全扩展要求。云计算、大数据、物联网和移动互联网等新兴技术与传统教育业务深度融合，为教育服务提供便利的同时引入了新的安全风险。

云计算技术帮助实现教育数据存储和管理，方便区域内教育机构数据交互共享，使用云计算技术存储和管理这些数据可以降低数据存储成本，提高系统性能和可扩展性。但是，云计算技术的使用使得教育数据、教育信息系统中心化，面临较多的网络攻击与刺探，一旦云平台出现问题，可能导致众多教育信息系统业务中断、教育数据丢失，影响教育活动的正常开展。

大数据技术可以对教育数据进行专业化分析和再利用，有效进行前瞻性预测及预警。但是，教育大数据具有隐私性强、可利用价值高、来源广泛的特点，在采集、传输、存储、应用、销毁等全生命周期内，教育大数据常常成为黑客重点攻击的目标，存

在 SQL 注入攻击、数据泄露的风险。

物联网技术帮助实现智能化教育，主要应用在教育场景构建、教育器材研发、教育素材创造、教育成效反馈、教育参与者数据采集等各方面，其数据具备一定敏感性，容易造成敏感信息泄露等问题。

移动互联网技术应用较多的是移动教育 App，这些 App 深入在线教学互动中，为教育信息展示、线上教育服务提供便捷途径。移动互联网教育网络安全风险主要体现在数据平台分散化，移动终端难以集中管控，移动数据公网裸奔，容易造成权限划分不明、敏感信息泄露等问题。

“互联网+教育”对传统教育模式进行了重大变革，在线教育平台与海量教育 App 方兴未艾。云计算、大数据、移动互联网、物联网、人工智能与 5G 通信等新技术的应用给教育行业引入的网络风险不可忽视，因此在“等保 2.0”时代更应当重视教育行业网络安全，通过网络风险评估、等级保护测评手段，落实教育行业关键信息基础设施保护工作，对教育信息系统进行安全运营，解决内在漏洞隐患、外部病毒攻击、DDoS 攻击频发、在线教育平台及 App 风险突出、教育信息泄露频发等问题，切实做好新时代下的教育行业网络安全保障工作。

网络空间安全测评工程技术中心

地　址：北京市海淀区紫竹院路 66 号赛迪大厦 4 层

传　真：86-10-88559332

手　机：86-18610932568（李世斌）

86-15011288947（李松恬）

邮　箱：lishibin@cstc.org.cn（白利芳）

lijing@cstc.org.cn（李松恬）