高校数字化网络安全保障体系建设需求研究

陈　航
浙江省网络空间安全协会　浙江　杭州　310000

摘　要：随着信息技术在教育行业的广泛应用和深度融合，在教育系统、教育设备、教育环境等纷纷融入信息化元素的同时，也加大了攻击者对于教育行业相关教育数据的关注程度和攻击面，使支撑教育教学的底层网络系统、业务系统等在网络安全面临的威胁也持续加大。本文分析了高校网络信息安全的现状及问题，结合等级保护要求、数据安全治理、基于大数据技术的安全监测和态势感知等几个方向给出建设建议。

关键词：智慧校园；网络安全防护；安全运营

引言

近年来，黑客入侵教务管理平台窃取或倒卖学生学籍信息、篡改学校网站造成不良影响、植入勒索病毒到大量校园网电脑终端等信息安全事件逐渐增多，部分案例甚至造成了很大的社会影响。

在此安全背景下，校园信息化建设应重点关注信息安全工作的投入及成果，并结合业务实际情况，制定切实可行的安全保障机制，降低系统攻击面、增强安全防范能力，整体提高校园网基础信息网络和重要信息系统的信息安全保护能力。

1 高校数字化转型面临的网络安全威胁

随着技术的不断发展，数字化转型已经成为高校发展的必然趋势。高校开始利用信息化来改善业务决策、增强创新。应用系统基于信息化能力承接业务需求，是高校业务在信息化环境中的投射。应用系统也成为教学需求和信息化技术最主要的结合点，以及智慧校园建设的关键，这也给应用安全提出了更高的要求。

1.1 快速交付带来的挑战

在数字化转型的背景下，应用开发、运维模式都开始向敏捷模式转变。在敏捷模式下，一个迭代往往在1~2周内完成，应用系统的开发、测试、部署是快速迭代并同时进行的，这对应用系统安全保障提出了更高的要求。

1.2 集成中间件的增加带来更多风险

在数字化转型的背景下，应用系统开发团队会更多地使用中间件来开发提升开发效率。由于中间件集成的增加，软件供应链对应用系统安全性的影响增大，这将给应用系统安全带来更多风险。

1.3 自动化带来全新的要求

在数字化转型的背景下，应用系统的开发、测试、运维都需要广泛地使用工具和平台来提升自动化水平。在这些应用系统的生命周期内引入的自动化的工具和平台，对安全融入应用系统生命周期提出了全新的要求。

1.4 应用系统的安全要求不断增强

在数字化转型的背景下，随着网络安全法、密码法、“等保2.0”的颁布，以及个人信息保护、数据安全相关标准和立法的不断推进，国家、教育主管部门对信息化的安全要求不断提升，对应用系统的安全要求也不断增强。与此同时，越来越多的应用系统随业务的发展不再局限于在校内使用，而更多地向合作伙伴、学生开放，这也将对应用系统提出了更高的安全要求。

2 高校信息系统安全风险及需求分析

2.1 安全技术风险分析

当今，信息化技术快速发展，新技术的应用促使校园信息化系统的业务模式也产生了很大变化，移动办公、虚拟化、大数据、云计算等新兴技术已经成当今高校信息化建设和提供服务的主要模式。新技术的应用并没有使信息系统更安全，相反，不仅传统的安全威胁依然存在，系统还面临着由于新技术、新服务模式的应用所带来的新的安全风险。

信息安全风险是资产、威胁和系统脆弱性三个因素共同作用导致的，信息安全风险评估是围绕着资产、威胁、脆弱性和安全措施这些基本要素展开的，在对基本要素的评估过程中，需要充分考虑业务目标、资产价值、安全需求、安全事件、残余风险等与这些基本要素相关的各类属性。

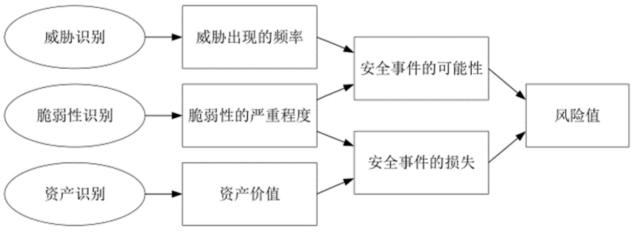

图1 信息安全风险分析的原理图

由三者之间的关系可以得出：

（1）业务目标的实现对资产具有依赖性，依赖程度越高，要求其风险越小；

（2）资产是有价值的，组织的业务目标对资产的依赖程度越高，资产价值就越大；

（3）风险是由威胁引发的，资产面临的威胁越多则风险越大，并可能演变成为安全事件；

（4）资产的脆弱性可能暴露资产的价值，资产具有的弱点越多则风险越大；

（5）脆弱性是未被满足的安全需求，威胁利用脆弱性危害资产；

（6）风险的存在及对风险的认识导出安全需求；

（7）安全需求可通过安全措施得以满足，需要结合资产价值考虑实施成本；

（8）安全措施可抵御威胁，降低风险；

（9）残余风险有些是安全措施不当或无效,需要加强才可控制的风险；而有些则是在综合考虑了安全成本与效益后不去控制的风险；

（10）残余风险应受到密切监视，它可能会在将来诱发新的安全事件。

以下通过威胁主体、来源、途径等多种属性分析校园网信息系统安全防护对象所面临的安全威胁。

2.2 通用安全风险

随着国家实施“互联网+”战略、各类互联网应用日新月异，传统的网络架构也发生了巨大变化，信息系统更加开放，面向更多的公众提供服务，接入网络更加复杂，终端分布范围更广且多样化，攻击者技术和手段不断提高，传统的安全架构和防护手段已经远不能应对新的安全风险，这些风险主要体现在：

（1）信息技术的快速发展使得安全边界不断扩大，传统安全架构面临挑战。

（2）局部分散的防护措施无法应对更加多样化的攻击手段，安全需具备体系化建设思想。

（3）攻击防不胜防，安全监测、预警、响应能力成为关键

（4）国家层面网络对抗不断升级，面临更严格的安全监管要求。

2.3 新技术新威胁带来的安全风险

2.3.1 远程及移动办公安全风险分析

校园OA围绕“无纸办公”、“协同办公”的电子政务理念，实现绿色环保“数字化”校园，大大提高学校行政人员的工作效率和工作质量，移动办公技术可以解决分校区或出差员工远程办公的问题。对于分支机构人员、经常出差的流动工作人员，可以随时随地、以费用低廉而安全可靠的联网手段使用校园本部的OA系统，及时查询信息和处理业务，极大提高行政办公效率。但移动终端往往处在不受控的办公环境中，通过互联网连接到校园网中，通过攻击移动终端及远程传输网络渗透到服务器系统导致信息泄露，资产被盗的例子举不胜举。

尤其在疫情期间，根据腾讯云安全、桌面安全、云鼎实验室等团队针对云上业务的网络攻击趋势解析如图，教育行业成黑客重点攻击对象。

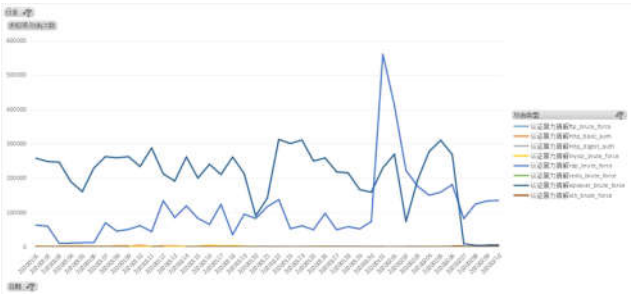

图2

春节前期是大多数高校的“封网”时期，也正是黑客的“骚动期”。据介绍，“封网”期间安全策略更新的时效性较平日差，因此引来黑客试图乘虚而入，攻击量达到高峰节点。

而在春节过后，众多高校开启远程授课模式，一本（字典）万利（权限）的认证暴力猜解成为黑客最常采用的攻击手段。

此外，移动APP的互联性和易用性使其暴露在众多的网络安全风险和威胁之下，容易遭受到病毒、木马、蠕虫等恶意程序的攻击，攻击者能够通过移动APP的安全漏洞入侵应用服务器，获取学校及个人用户的敏感信息，或通过技术手段对应用程序进行篡改，植入广告、盗链及数据窃取等功能，甚至对数据进行篡改，对信息系统进行恶意破坏，保护移动APP安全刻不容缓。

2.3.2 虚拟化技术安全风险分析

虚拟化技术是生成一个和真实系统行为一样的虚拟机器，虚拟机像真实操作系统一样，同样存在软件漏洞与系统漏洞。在关注宿主机的安全的同时，必须像对待真正的操作系统一样加固虚拟机，给程序不断地及时打补丁升级，以此来保证虚拟机的安全。

虚拟机之间的隔离主要通过虚拟化层软件实现，软件的漏洞为攻击者提供了方便之门。虚拟机镜像、快照恢复的时候，由于缺乏及时的系统补丁，造成新创建的虚拟机极易受到攻击。

此外，传统网络可以通过交换机、IDS等设备进行日

常监测、审计，而虚拟主机间可能通过硬件背板而不是网络进行通讯，这些通讯流量对标准的网络安全控制来说是不可见的，因此，传统的安全防护措施变成了毫无用处。

由于虚拟化环境自身的特性，单位需要充分考虑虚拟化的引入所带来的相应的风险，根据各个风险点带来的问题及威胁建设针对性的防护方案，以保障单位数据的安全及业务系统的平稳运行。

2.4 新型攻击带来的安全风险分析

高级持续性威胁（Advanced Persistent Threat，以下简称“APT攻击”）是一种典型的新型攻击模式，甚至已经成为当今各国面临的主要的信息安全威胁，其造成的破坏性和带来的危害远大于普通的安全事件。

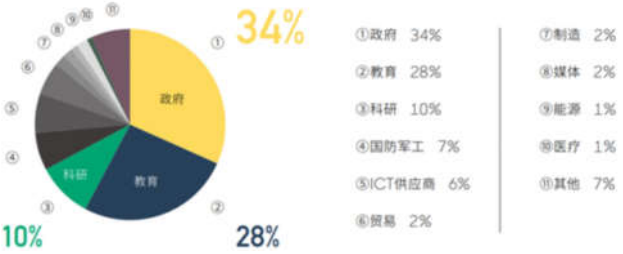

图3 2021年上半年中国地区受影响行业分布

政府、教育、科研是重灾区，受攻击影响占整体超七成。另外医疗、媒体威胁凸显；

APT攻击可以绕过各种传统安全检测防护措施，通过精心伪装、定点攻击、长期潜伏、持续渗透等方式，伺机窃取网络信息系统核心资料和各类情报。事实证明，传统安全设备已经无法抵御复杂、隐蔽的APT攻击。

传统安全防御体系的框架一般包括：接入控制、安全隔离、边界检测/防御、终端防御、网络审计、访问控制等，所涉及的安全产品包括：防火墙、IDS/IPS、杀毒软件、桌面管理软件、网络审计、双因素认证等。而APT攻击，其采用的攻击手法和技术都是未知漏洞（0day）、未知恶意代码等未知行为，在这种情况下，依靠已知特征、已知行为模式进行检测的IDS、IPS在无法预知攻击特征、攻击行为模式的情况下，理论上就已无法检测APT攻击。

在国家新等级保护标准中，明确提出了“应采取技术措施对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析”，就是应对当前信息安全威胁的新形势而提出的新的安全防护要求，需采取有效的防护手段应对新的安全风险。

2.5 安全管理风险分析

信息系统在建设和运营过程中，都面临着安全管理缺失带来的安全风险。

2.5.1 系统建设期面临的安全管理风险

新系统的开发、新技术的应用、新的应用模式都加大了信息安全管理层面的难度和风险。

首先，新系统开发时间紧，任务重，人员队伍建设无法迅速满足系统建设的需求，在很多环节导致安全管理上的缺失和不足，如应用系统在规划设计阶段未充分考虑安全功能的需求，导致系统在上线交付时无法满足安全要求，而系统已经开发完成，任何针对信息系统的重新设计或功能完善都将导致迭加的成本投入，甚至不可行。而在应用系统的整个开发过程中，代码编写不规范、人为设置的系统后门开发过程安全管理都是不可忽视的问题，如果不进行规范管理，将导致系统上线后的各种安全问题。

其次，虚拟化、大数据、移动办公等新技术、新应用模式的使用，要求信息安全管理人员能充分认识到信息技术可能带来的安全技术风险和安全管理风险，传统的安全管理手段需要在新技术下进行调整和优化，如针对移动办公，安全管理边界明显扩大，安全管理要求必须配备技术手段的应用；此外，海量敏感信息数据也需要严格的安全管理措施，在系统投入运营前，严格控制采用实际数据进行系统测试，并采取严格的人员管理措施。

2.6 系统运营期面临的安全管理风险

系统投入运营后面临来自组织层面和系统运营层面的安全管理风险。

（1）组织层面的安全管理包括安全策略、安全制度体系的建设和完善以及安全管理机构的建设和人员安全管理。首先，信息安全管理需要明确的安全管理机构和专职的安全管理人员，目前，许多单位已经建立了比较完善的安全管理机构，并且配备了专职的安全管理人员，但随着系统规模的不断扩大，新上线系统的不断增加，人员不足已经成为普遍的问题，此外，内部人员的信息安全意识水平需要不断提高，事实证明，很多网络信息安全事件都是由于内部人员的疏忽或恶意行为导致的。

其次，随着高校信息化的快速发展，信息安全技术体系的不断完善，原有的安全管理策略和制度也需要不断完善，“三分技术、七分管理”，体现了信息安全管理的重要性，安全管理制度要体现和落实安全管理责任制，形成由安全策略、管理制度、操作规程、记录表单等构成的全面的信息安全管理制度体系，并切实执行落地。

（2）系统运营层面的安全管理包括办公环境管理、资产管理、介质管理、设备维护管理、系统变更管理、配置管理、备份和恢复管理、应急管理等，体现在系统

运营过程中的各个方面，运营管理的缺失可能导致信息系统崩溃、数据泄露、丢失、设备损害等风险，运营安全管理往往需要辅助技术手段措施，完善各操作环节的规章制度、完善安全配置基线，进行操作培训、安全培训、应急演练、备份与恢复演练。

2.6.1 系统运营风险分析

系统投入运营后，面对数量庞大的信息资产、海量的日志信息和复杂多变的策略体系，日常安全运营存在较大安全隐患和风险，主要表现在：

（1）数量庞大的资产信息无法完全掌控

校园网信息系统的网络和业务越来越复杂，范围原来越广，变更越来越频繁，安全管理员也常常搞不清楚内网的具体状况，如，哪些资产是关键资产，哪些资产对外提供服务，哪些资产配置了安全策略等，如果连这些单位内网的基本环境都无法准确掌握，那就更谈不上对内部网络、资产的安全风险的掌握了。在这种情况下，攻击者即便是大摇大摆的出入高校的敏感数据区域也无人知晓，投入了大量资金建设的安全防御体系也成了摆设。因此，需要通过自动化的手段掌握全网的资产状况，这也是系统安全运维的基础。

（2）分散多样的信息设备对策略的维护是巨大挑战

随着网络基础建设和网络安全控制的逐步健全，高校的网络环境规模和复杂度不断增加，部署在其中的防火墙以及配置访问控制列表的路由交换设备日益增多。新的运维应用场景需求不断新增，加载于这些设备之上的网络安全策略规则也相应的变得更加繁冗和复杂。此外，实际的网络环境中，往往会跨越多个供应商、多个运维团队，管理控制方面呈现出多分支、多层级的复杂局面。策略控制的粒度日趋细化严格，网络复杂度不断增加导致运维效率更加底下，两者之间的矛盾在实际运维中会日趋明显。传统的依赖于人手动维护网络设备管理方式将变得越来越无法容忍，且带来的运维成本不断增加。

（3）高级威胁和未知病毒的检测和分析考验专业运维能力

图4 APT攻击的原理图

随着攻击对抗技术的不断发展，越来越多的信息安全事件是由长期持续、有组织的高级威胁和未知病毒所导致的，而面对这类问题，普通运维人员往往束手无策，攻击者的手段和变化形式越来越多样化，带来的危害也越来越大，仅依靠普通驻场运维人员很难定位和解决这类安全问题，一旦安全事件得不到定位分析和处置，持续蔓延将可能造成重大损失，因此，在系统运营过程中，是否有及时发现问题的一线运维人员，以及能进行专业分析定位安全问题的技术专家是安全运维能力的集中体现，也是安全运营的重要因素。

（4）面对安全事件的快速响应是安全运营的关键

本地化安全运维能确保对安全事件的应急响应速度，面对信息安全事件，快速响应和处置的能力体现在应急专业队伍的技术水平、应急服务网络的覆盖度、应急流程和体系的成熟度以及应急响应经验和资源准备情况等，针对金华理工学院校园网信息系统庞大的网络结构和资产数量，专业的应急队伍和应急支撑平台的建设是降低系统运营安全风险的必要措施，系统运营中应急技术能力的建设包括了人员、工具、设备、流程、系统平台等多种因素，其中，专业人员是关键，但仅有人员，没有相关的设备、工具、应急指挥系统、应急预案等也无法提升系统运营过程中的应急响应能力，各因素缺一不可。

2.7 系统安全需求分析

2.7.1 安全技术需求分析

面对来自信息系统内外部的各种安全威胁，以及新技术新安全形势的发展，需要从多层级、多维度建设整体的、符合系统安全保护等级要求的安全防御体系。

具体安全技术需求如下。

2.7.2 物理环境安全需求

物理和环境安全主要是指由于网络运行环境和系统的物理特性引起的网络设备和线路的不可使用，从而会造成网络系统的不可使用，甚至导致整个网络的瘫痪。它是整个网络系统安全的前提和基础，只有保证了物理层的可用性，才能使得整个网络的可用性，进而提高整个网络的抗破坏力。

物理和环境安全包括机房选址、机房建设、设备设施的防盗防破坏、防火、防水、电力供应、电磁防护等，需要在数据中心机房的建设过程中严格按照国家相关标准进行机房建设、综合布线、安防建设，并经过相关部门的检测和验收。

2.7.3 通信网络安全需求

网络整体架构和传输线路的可靠性、稳定性和保密性是业务系统安全的基础，通信网络的安全主要包括：网络架构安全、通信传输安全、边界安全、防入侵、网络安全审计和网络安全的集中管控等方面。

2018-2022年，1920所高校的网络出口校均带宽由

6.8G/校提升至12.2G/校，校均网络出口带宽的年均增长率为15.7%。

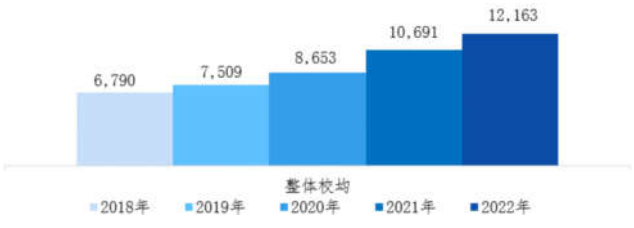

图5 2018–2022年高校校均网络出口带宽（IPv4+IPv6）（单位：M/校）

（1）网络架构安全

网络架构是否合理直接影响着是否能够有效的承载业务需要。因此网络结构需要具备一定的冗余性；带宽能够满足业务高峰时期数据交换需求；并合理的划分网段和VLAN。

（2）通信完整性与保密性

由于网络协议及文件格式均具有标准、开发、公开的特征，因此数据在网上存储和传输过程中，不仅仅面临信息丢失、信息重复或信息传送的自身错误，而且会遭遇信息攻击或欺诈行为，导致最终信息收发的差异性。因此，在信息传输和存储过程中，必须要确保信息内容在发送、接收及保存的一致性；并在信息遭受篡改攻击的情况下，应提供有效的察觉与发现机制，实现通信的完整性。

而数据在传输过程中，为能够抵御不良企图者采取的各种攻击，防止遭到窃取，应采用加密措施保证数据的机密性。

2.7.4 区域边界安全需求

（1）边界隔离与访问控制

边界安全包括对接入网络和外联的双重安全管控要求，随着移动办公的发展，网络范围不断延展，无线网络的使用相对传统办公而言，对网络边界的有效管控更是严峻的考验；对于一个不断发展的网络而言，为方便办公，在网络设计时保留大量的接入端口，这对于随时随地快速接入到业务网络进行办公是非常便捷的，但同时也引入了安全风险，一旦外来用户不加阻拦的接入到网络中来，就有可能破坏网络的安全边界，使得外来用户具备对网络进行破坏的条件，由此而引入诸如蠕虫扩散、文件泄密等安全问题。因此需要对非法客户端实现禁入，同时，需要能够对内部用户非授权联到外部网络的行为进行限制或检查；并对无线网络的使用进行管控。

（2）防入侵和防病毒

现今，病毒的发展呈现出以下趋势：病毒与黑客程序相结合、蠕虫病毒更加泛滥，目前计算机病毒的传播途径与过去相比已经发生了很大的变化，更多的以网络形态进行传播，并且，一旦病毒通过网络边界传入局域网内部，就已经对信息系统造成了破坏，因此，病毒防护手段需要在系统边界进行部署，在网络层进行病毒查杀，防止感染系统内部主机。

此外，来自互联网、其他非可信网络的各类网络攻击也需要通过安全措施实现主动阻断针对信息系统的各种攻击，如病毒、木马、间谍软件、可疑代码、端口扫描、DoS/DDoS等，实现对网络层以及业务系统的安全防护，保护核心信息资产的免受攻击危害。

（3）网络安全审计

安全技术措施并不可能万无一失，一旦发生网络安全事件，需要进行事件的追踪与分析，针对网络的攻击行为和非授权访问等行为，需要在网络边界、重要网络节点上进行流量的采集和检测，并进行基于网络行为的审计分析，从而及时发现异常行为，规范正常的网络应用行为。

2.8 计算环境安全需求

信息设备存储和处理大量的业务信息，也是攻击者的最终目标，主机系统自身的漏洞一旦被攻击者利用，获取系统权限，将直接导致信息系统被破坏或数据泄露。此外，应用和数据是安全保护的对象，应用系统在开发过程中由于技术的局限性和开发管理的漏洞，总是存在一些安全漏洞，在系统上线后，被恶意攻击者利用，进而给单位的经济利益、业务、甚至声誉带来影响。

计算环境安全需求包括对主机和应用系统用户进行身份鉴别和访问控制、安全审计、对主机和各类终端的入侵防范和恶意代码防护、数据保密性和完整性保护、数据备份与恢复、剩余信息和个人信息保护。具体包括：

（1）主机身份鉴别

主机操作系统登录均必须进行身份验证。过于简单的标识符和口令容易被穷举攻击破解。同时非法用户可以通过网络进行窃听，从而获得管理员权限，可以对任何资源非法访问及越权操作。因此必须提高用户名/口令的复杂度，并定期进行更换，或者，采取更可靠的身份鉴别措施。

（2）主机访问控制

主机访问控制主要为了保证用户对主机资源的合法使用。非法用户可能企图假冒合法用户的身份进入系统，低权限的合法用户也可能企图执行高权限用户的操作，这些行为将给主机系统带来了很大的安全风险。用户必须拥有合法的用户标识符，在制定好的访问控制策

略下进行操作，杜绝越权非法操作。

（3）系统审计

对于登陆主机后的操作行为则需要进行主机审计。对于服务器和重要主机需要进行严格的行为控制，对用户的行为、使用的命令等进行必要的记录审计，便于日后的分析、调查、取证，规范主机使用行为。

（4）恶意代码防范

病毒、蠕虫等恶意代码是对计算环境造成危害最大的隐患，当前病毒威胁非常严峻，特别是蠕虫病毒的爆发，会立刻向其他子网迅速蔓延，发动网络攻击和数据窃密。大量占据正常业务十分有限的带宽，造成网络性能严重下降、服务器崩溃甚至网络通信中断，信息损坏或泄漏。严重影响正常业务开展。因此除了在网络层采取必要的病毒防范措施外，必须在主机部署恶意代码防范软件进行监测与查杀，同时保持恶意代码库的及时更新。

（5）应用系统安全功能开发

应用系统在开发过程中需同步考虑安全功能的实现，包括系统用户管理、身份认证、访问控制和应用安全审计等相关功能，并在应用系统开发过程中通过采用密码技术实现数据的完整性和保密性保护。

需要实现对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换；对于重要信息系统需要采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现；

需要提供访问控制功能，对登录的用户分配账号和权限；授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；访问控制的粒度应达到主体为用户级，客体为文件、数据库表级、记录或字段级。

需要提供安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

需要提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；在故障发生时，应自动保存易失性数据和所有状态，保证系统能够进行恢复。

需要提供剩余信息保护功能，保证释放内存或磁盘空间前，上一个用户的登录信息和访问记录被完全清除或被覆盖。

（6）数据完整性与保密性

数据是信息资产的直接体现。所有的措施最终无不是为了业务数据的安全。因此数据的备份十分重要，是必须考虑的问题。具体包括：

需要采用校验码技术或密码技术保证重要数据在传输和存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

采用密码技术保证重要数据在传输和存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

（7）数据备份和恢复

对于关键数据应建立数据的备份机制，而对于网络的关键设备、线路均需进行冗余配置，备份与恢复是应对突发事件的必要措施。

2.9 集中安全管控需求

信息系统内部署着大量的安全设备和网络设备，各安全设备和网络设备每天采集大量的日志信息和流量信息，需要对设备进行统一的、集中的管控，包括以下几方面：

（1）安全管理实现三员分离

具备系统管理、安全管理和审计管理功能，功能权限分离，三员（系统管理员、审计管理员、安全管理员）分离，并能对三员进行身份鉴别和操作审计。

（2）统一安全运营和管控的需求

对于资产规模和部署范围庞大的校园网系统，必须建设统一的安全运营和管理中心，对全网资产、日志、事件信息进行统一的监测、检测、响应和分析，掌握全网的信息资产安全状况，及时发现和处置安全事件。

（3）集中安全策略管理需求

面对复杂的网络结构，多厂商安全设备，由人工进行安全策略的配置和动态调整，无论是从工作量和工作难度上来说都是不可接受的，需要能够采用自动化工具进行全网主要设备的安全策略自动下发和集中管理。

3 安全管理需求分析

根据上述的针对建设期和运营期的安全管理风险分析，总结以下安全管理需求：

3.1 建设期安全管理需求

系统建设期包括系统的系统设计阶段、系统开发设计阶段、系统工程实施阶段、系统测试验收阶段和系统交付阶段，在整个建设期间需要加强以下安全管理：

（1）系统规划设计阶段需同步安全设计

在应用系统的需求分析阶段就需要同步考虑安全需求，并进行安全功能的规划和设计，并且在信息系统建设规划阶段，也需要同步考虑安全技术体系的设计，并

在应用开发和系统建设过程中同步落实相关安全措施，对安全产品和密码产品的选型要符合国家等级保护的相关要求。

（2）需加强外包软件开发管理

外包软件开发面临来自人为的恶意和非恶意的安全风险，数据表明，大部分软件开发都不可避免地存在代码漏洞，但严格的安全开发管理能大大降低应用系统漏洞带来的风险，因此，需要在外包软件开发过程中加强对开发人员、开发过程、编码规范、代码审查管理，并要求外包厂商提供源代码。

（3）工程实施安全管理

在整个工程实施过程中，需要指定专门的部门和人员负责工程实施过程管理，指定工程实施方案控制安全工程实施过程，并引入第三方监理控制项目的实施过程。

（4）系统测试验收和交付管理

在系统正式上线前，需要进行必要的系统测试，制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；需要进行上线前的安全性测试，并出具安全测试报告。在系统交付过程中，需制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；对负责运行维护的技术人员进行相应的技能培训；确保提供了建设过程中的文档和指导用户进行运行维护的文档。

（5）系统测评和服务供应商选择

按照等级保护的要求，三级信息系统必须经过国家等级保护测评，并对不符合项进行整改，对服务供应商的选择需要符合国家的有关规定。

3.2 运营期安全管理需求

运营期指系统上线投入运营后到系统废止，运营期安全管理需要建设一整套信息安全管理体系并加以落实，按照等级保护和ISO27001的信息安全管理体系建设要求，信息安全管理文件体系包括信息安全方针和策略、信息安全制度、操作流程和规范、记录表单等分层级的信息安全管理制度系统，其中，每一层级文件都是对上一层级的具体化和落实，从安全管理体系构成来说包括安全管理制度、安全管理机构、安全管理人员、安全运维管理等几个方面，每个方面都需要制定和落实相关的管理制度，信息安全制度体系与信息安全技术体系和信息安全运营体系相辅相成，缺一不可。

3.3 高校负责网络安全工作的人员配置情况

我国1998所高校在负责网络安全工作的专职人员方面，有34.5%的高校没有专职人员负责，由其他岗位兼职；52.5%的高校有1-2人负责；3人及以上的占比13%。

从高校类型上看，“双一流”高校的网络安全专职人员配置相对较多，分别有65.6%和21.0%的高校选择了“1-2人”和“3-5人”，其校均人员配置约为2人；普通本科与整体分布差异不大，选择“1-2人”和“无，其他岗位兼职”分别占比55.1%和32.3%；高职高专和成人教育选择“无，其他岗位兼职”的院校占比相对更高，分别为42.2%和41.2%。

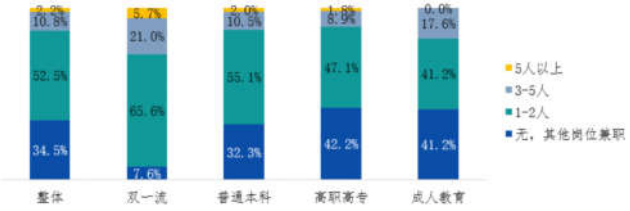

图6 高校负责网络安全的人员配置

3.4 高校网络安全服务需求

在高校网络安全服务需求方面，五成以上高校的网络中心老师认为通过安全防护、安全检测、安全加固、重保与应急等服务可以为学校的网络安全工作带来帮助。

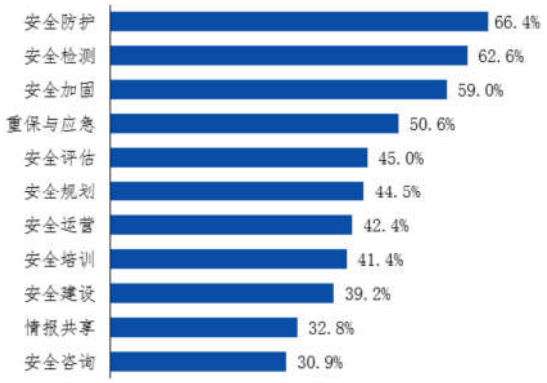

图7 高校网络安全服务需求

4 安全运营需求分析

安全运营需求分析从技术角度分析系统上线运行后在整个较长的后续运营期间对安全运营的需求。主要包括：

（1）全面掌握信息安全资产需求

信息安全运营的前提是摸清网内信息资产的全貌，这些资产包括主机/服务器、安全设备、网络设备、WEB应用、中间件、数据库、邮件系统和DNS系统等，资产的信息包括设备类型、域名、IP、端口、版本信息等，这是信息安全运营的前提和基础，而单位往往并不完全掌握这些资产信息，采用人工方式进行资产梳理对于庞大的信息系统既不可能，也不全面，因此，首先需要进行全网信息资产的自动化发现，并结合业务特点，对资产的重要性等情况进行梳理，形成资产清单，并能对变化进行周期性的监控。

（2）日常安全运营需求

单位信息系统在上线后，需要对网络及系统进行日常安全运维，包括定期的系统安全评估、检查系统的配置是否满足安全防护的需求，定期检查设备的运行状态和系统漏洞情况，及时修补系统漏洞，对于应用系统新上线的功能模块或新上线系统进行安全评估、代码审计，并在上线后定期进行渗透测试，针对于暴露于互联网的WEB应用由于其面临的风险更大，还需要提供更专业更实时的运维服务支撑。

（3）重要时期安全保障需求

对于教育行业，高校在重要时期的安全运营保障服务尤为重要，是领导关注的重点工作。重要时期的安全运营保障包括了事前、事中、事后的整体的安全运营保障服务，需要更加全面的安全评估检查、渗透测试，以及应急演练，现场值守、应急处置和后续的工作总结等。重要时期的安全保障能力集中体现了单位安全运营的能力水平。

结束语

属于数字化高校的时代已经到来，数字化高校正在回应国家、社会和个人对高等教育提出的期望，在满足这些不断增长的高等教育期望的同时产生了非凡价值。同时，当前安全威胁形势已经发生了很大的变化，大部分安全事件都是由于未知威胁或高级安全威胁导致的，如近两年发生的勒索病毒事件，单位内部的安全团队面对这样的威胁形势往往束手无策，一旦发生安全事件，如果无法及时处置，将导致不可估量的损失，这些损害不仅仅是经济层面的，还伴随着大量敏感数据的泄露。

因此，新等级保护制度增加了单位对于未知威胁的检测、发现和分析能力的要求以及对日志的综合分析能力的要求，对于关键信息系统需要有专家级的安全分析和应急响应能力，在安全事件发生时，能将事件造成的损失和影响降至最低，并对事件进行分析溯源，防患于未然。

当数字化高校改变了终身学习时代的高校和高校的未来，网络安全保障体系建设将为我们崭新的数字化高等教育体系保驾护航。

参考文献

[1]“十四五”高校信息化思维创新与路径选择。胡钦太-《中国教育网络》-2021

[2]国际21世纪教育委员会.Learning:The Treasure Within [R].美国：国际21世纪教育委员会,1996.

[3]林建华.大学的改革与未来[M].北京：东方出版中心,2018.

[4]张文刚.基于数字化校园综合安防管理系统的设计[M/CD].中国学术期刊电子杂志社,2007,3.