信息化摘编 NO.20

2023-12-20 东师信息化办

本期导读

汇 高校信息化新业态

聚 兄弟院校之优长

高校信息化新业态

一．全球高等教育网络安全发展新态势

高校作为知识的摇篮和科技创新的重要场域，其网络安全问题受到持续且密切的关注。今年以来，国外政府及高校纷纷采取针对性措施，推动网络安全建设进入常态化轨道，以保障教育、研究和创新的顺利开展。

1. 国家层面：推动高校网络安全常态化

①英国提出高校数据保护政策

近日，英国政府提出了一系列针对高校的个人数据保护和数据泄露应对政策，旨在指导高校遵守数据保护法、制定数据保护政策和流程、明确教职工和学生数据的保留要求、遵守个人数据泄露防范准则。

②美国将支持高校网络安全研究

根据去年颁布的《芯片和科学法案》，美国国家标准与技术研究院（NIST）考虑为高校提供支持网络安全研究的资源。美国高等教育信息化协会 EDUCAUSE 提出建议，鼓励 NIST 与高校网络中心合作，建立在线信息库，集中提供有关高校及其现有资源的信息，以便师生更易获取研究网络安全信息和支持的相关知识。同时，还建议 NIST 为高校学术研究人员及其团队提供通用的网络安全资源，协助他们在研究中确立网络安全标准，以满足研究领域的重要需求。另外建议 NIST 可以利用其作为主要联邦科学研究机构的地位，强调并支持高校网络安全专业发展途径，促进网络安全领域进一步发展。

③澳大利亚指导高校网络安全

澳大利亚网络安全部长克莱尔 •奥尼尔宣布制定《2023-2030 年澳大利亚网络安全战略》。澳大利亚教育部在高校网络安全指导方针中建议高校采取以下措施以确保网络安全：

第一，利用网络威胁模型，了解并按比例降低风险；第二，实施大学网络安全战略；第三，将网络安全作为整个组织的“人”的问题，大力强调安全文化；第四，加强澳大利亚大学的网络安全项目。

2. 高校层面：全方位服务师生网络安全防御

①哈佛大学生成式 Al 安全指南：生成式 AI 风靡全球，但哈佛大学一直对其抱有谨慎态度，并特别关注其如何保护数据的安全性。2023 年 9 月，哈佛大学文理学院发布了在课

堂中使用 ChatGPT 等生成式 AI 的使用指南，该指南建立在 7 月哈佛大学本科教育办公室发布的“哈佛全校人工智能指南”基础上，重点保护非公开数据的安全。

②斯坦福大学多维度安全服务：为保障校园计算机资源和数据的安全，斯坦福大学的 IT 部门提供了一系列服务和工作，旨在满足师生们的网络安全需求，其中包括桌面配置、移动设备管理、身份验证系统、反恶意软件、防火墙和网络监控等。

以下是斯坦福大学主要的网络安全服务：

反恶意软件服务：学校为各类计算机设备提供 CrowdStrike Falcon 反恶意软件服务，用于保护计算机免受病毒、广告软件、间谍软件和其他恶意软件的侵害。

设备注册：为确保只有身份明确的用户能够访问斯坦福数据，每位用户都需要完成简单的注册过程，以将其身份与每台设备相关联。

安全电子邮件服务：专为斯坦福大学成员设计，根据 HIPAA 准则使用电子邮件传输受保护的健康信息（PHI）。

端点合规性报告：为系统和部门管理员、本地桌面支持和管理人员提供信息，以监控连接到斯坦福网络的设备是否合规。

端点配置管理（BigFix）：通过自动进行操作系统和其他常用软件的安全更新确保计算机的安全。

文件完整性监控（OSSEC）：监控文件完整性，记录服务器文件系统的更改，帮助检测和调查入侵或文件更改。

文件存储安全：使用自动工具扫描文件共享系统中存储的文件，以查找可能被可公开访问且包含高风险数据的文件。文件所有者将通过电子邮件收到关于更改的通知，而后能够根据需要更新文件共享权限。

移动设备管理（AirWatch）：移动设备管理（MDM）允许用户通过斯坦福大学的网络工具管理移动设备，并生成配置文件，以确保其安全访问内部系统，同时保护设备上的数据。

我的设备（MyDevices）：可让学校附属机构查询与其相关的设备，并查看这些设备是否已使用可验证的加密进行保护。

网络钓鱼防范意识服务：通过模拟网络钓鱼电子邮件，培训参与者识别、报告和避免网络钓鱼攻击。

③麻省理工学院安全软件服务：学校鼓励师生安装 Sophos Anti-Virus 和 CrowdStrike Falcon；推荐使用 LastPass 等密码管理器；提供了基于云的备份解决方案，使用 CrashPlan 备份电脑数据；建议安装 Spirion；提供了多种许可的企业视频会议工具，如 Zoom、Microsoft Teams 和 Webex 等，以确保用户的隐私安全。

④耶鲁大学校园网络安全活动：学校将常用服务的风险分为高、中、低三个等级，并倡导师生了解网络钓鱼的术语，定时检查更新系统，以确保网络安全。此外，耶鲁大学还积极开展了使用安全密码的教育活动，指导大家分辨安全密码和潜在风险密码。

耶鲁鼓励师生订阅网络安全意识的月度提示，即 Bee Cyber Fit Monthly Tip，提供定期的骗局揭示、故事分享、新闻更新和安全建议，同时鼓励大家分享遇到的网络骗局，形成网络安全防护意识，持续提醒大家时刻保持警惕，共同维护网络安全。

⑤剑桥大学师生网络安全培训：学校要求师生完成网络安全培训；学校提供免费的杀毒软件；还建立了计算机安全事件响应小组，提供网络安全测试、防火墙管理、入侵防御系统、英国 GDPR 系统清单及信息和网络安全战略等服务，会迅速报告 IT 安全事件，将对大学造成的损失降到最低。

⑥帝国理工学院使用 MFA：学校制定了信息系统安全政策，该政策覆盖信息管理各方面，并提出了关于信息保护的具体意见。要求师生必须了解并遵守该政策，并为进一步加强信息保护，学校为每个部门都配备了一名本地数据保护协调员，他们将成为用户数据保护查

询的首要联系人。对于那些未能妥善保护信息或滥用系统的师生，学校将会采取严厉措施，情节严重者或面临开除或承担法律责任的后果。此外，学校要求师生在登录系统时使用多因素身份验证即 MFA（Multi-Factor Authentication），这意味着在输入密码后需要提供额外的身份验证信息，以提高账户的安全性，确保只有授权用户能够访问。

⑦墨尔本大学鼓励访问安全网站：学校鼓励师生定期访问 ACSC；Scamwatch；Stay Smart Online；电子安全专员办公室网站，随时获取关于网络安全的最新资讯，实现安全上网。

⑧悉尼大学投入大量资源：学校遵循最佳实践网络安全标准，建立了明确的政策框架，并在网络安全计划中投入大量资源。网络安全政策明确规定了保护大学内部 ICT 资源和数字信息的保密性、完整性和可用性所需的责任和原则。此外，信息和通信技术资源可接受使用政策则适用于大学信息和通信技术资源的所有用户，概述了用户的权利和责任、大学信息和通信技术服务的使用条件及对滥用行为的处罚。

学校会定期发布网络安全建议，以确保师生随时了解当前存在的网络威胁。同时，学校鼓励师生随时报告任何网络安全事件，包括但不限于怀疑 ICT 服务、设备或账户受到威胁，发现有证据表明大学 ICT 服务存在漏洞，未经授权披露敏感信息或发现学校资产丢失，发现有人违反学校政策。学校将在网络威胁危及校园数据安全之前迅速采取措施。

（信息来源：https://mp.weixin.qq.com/s/eAkD3xyEE87EXDlIP-vQQg）

二．数字化时代 高校探寻网络安全新思路

高校需要积极采用新的网络安全技术和方法，加强与外部机构的沟通和协作，共同构建一个更加安全、可靠、智能的网络安全防护体系。越来越多的高校意识到，“单兵作战、大刀长矛”的防御模式已经无法满足目前网络安全的需要。不断寻求适配的创新安全策略和技术，提升监测预警和快速应急响应能力，才是决胜网络安全战役的关键。我国大部分高校的网络安全工作即将进入新的时期：从保障等保、密评、数据安全等合规性建设，向推动制度、措施、人员综合实战化运营过渡。

1. 数字化新挑战：数据安全迫在眉睫

数据资源是数字化转型的核心要素之一，平衡好数据保护与应用发展、建立数据安全治理体系，是高校数字化转型亟待解决的关键问题。但就目前来看，高校对数据安全治理缺乏方法论的研究，设计和实施路径仍不够清晰，这就为数据泄露事件频发埋下隐患。

为此，我们必须正视数据安全所面临的具体挑战：包括缺乏统一的数据治理监控管理体系、数据安全产品和机制面临新的挑战、环境变化和经济社会发展变革带来了新的挑战。并在此基础上，体系化防御数据安全风险，做到有的放矢。

2. 安全即服务：校网安拥抱新范式

在全球数字化浪潮之中，我国高等教育也面临着较为多样的网络攻击，从去年 9 月西北工业大学遭受境外网络攻击，到今年 7 月国内多所高校 DNS 服务器遭受定向攻击，都在为我国高校网络安全工作敲响警钟。

越来越多的高校意识到：我们不得不采取一系列措施来防范和检测这类攻击，不能仅满足于等保合规建设，更需要综合性的网络安全措施和不断创新的安全策略。

首先，高校要走出孤军奋战的固化思维和战略模式，团结国家、教育部、企业、其他高校等第三方力量来应对外部攻击。

其次，高校需要积极采用新的网络安全技术和方法，加强与外部机构的沟通和协作，共同构建一个更加安全、可靠、智能的网络安全防护体系。这一支援系统既要有向内的“智能化”的安全运营系统，还应该有“常态化、体系化、实战化”的安全保障机制。

第三，网络安全托管云服务模式（MSS）正在成为高校更愿意尝试的新型模式。这标志着网络安全从单纯的产品购买转向了服务购买，不仅可以提高系统安全性能，还降低了信息

化部门管理和维护的负担。

最后，高校修建的网络安全“马奇诺防线”需要实战检验，攻防演练常态化才能真正决胜千里。通过定期深度体检，才能知道网络安全工作到底做得怎么样，存在什么样的短板。

3. 新技术防御：魔高一尺，更须道高一丈

积极跟踪应用新技术，对于学校应对层出不穷和不断升级的网络安全问题而言，至关重要。

①XDR 技术：一颗闪耀的新星

在高校网络安全领域，XDR（Extended Detection and Response，扩展检测与响应）技术成为引人注目的新兴技术。

XDR 可将多种安全产品原生集成的安全威胁检测和事件响应产品品类。该技术通过采集网络侧（N）+终端侧（E）的遥测数据进行深度关联分析，为用户呈现一个事件的完整攻击链，帮助用户快速完成事件检测和响应工作，避免陷入海量告警、误报、漏报问题中。还有很重要的一点是，这种主动方案还能跨网络、端点以及云基础架构提供数据的可见性，以应对日新月异的攻击技术。

高校运用 XDR 技术可以从三个方面实现对高校网络安全的优化：一是泛化聚合，泛化和集中处理端点、网络、应用、云基础设施等数据，并将安全数据和告警关联到事件；二是提高精度，通过多安全产品深度关联提高检测精度；三是关联响应，为基础设施控制点（即网络和端点）的响应提供协同联动的自动化能力，降低重复性任务，提高效率。

②AI 应用：网络安全防御的双刃剑

近年来，AI 在网络安全领域的应用，已经成为安全能力落地、发挥网络安全防御有效性，以及对抗 APT 等高级威胁的最直接、最关键的路径之一。无论是防守方还是攻击方，都会因为 AI 而变得反应更快，能力更强。

对于高校而言，AI 被广泛应用于安全态势感知、威胁情报分析、网络攻防对抗等领域，可以帮助实现极早期监测预警和快速应急响应。但在各种利益驱动下，攻击者也在学习和拥抱 AI，利用其产生更智能、更隐蔽的攻击方法和路径。

最近，关于如何充分发挥 ChatGPT 在安全领域的价值，备受关注。AI 大模型在网络安全领域的最佳应用场景几乎都来自安全运营，涵盖了从事件检测、调查、响应到汇报的各个环节。

总的来说，网络强校肩上挑，安全之事本无小，高校网络安全任重道远。

（信息来源：https://mp.weixin.qq.com/s/1bWx8kgtD3UKUu4I6y61WQ）

兄弟院校之优长

一. 我校与自治区党委网信办联合举办网络举报校园宣传活动（新疆大学）

为加强青少年网络安全教育，引导大学生群体文明上网、健康上网、安全上网，积极参与互联网违法不良信息举报，共同营造清朗校园网络空间。2023 年 9 月 20 日中午，我校党委网信办与校团委联合自治区党委网信办在红湖校区大学生活动中心东门外举办了“网络举报 E 起来”主题网络安全宣传活动。

本次活动通过发放宣传手册和现场讲解案例等方式，为学生们进行网络辟谣科普教育，普及了传播谣言的危害、识谣辨谣的方法，以及造谣传谣所需要承担的法律责任等内容。以此引导广大学生提高网络安全意识，倡导发现网络违法和谣言信息要积极举报，构建清朗网络空间，形成文明健康的网络生活方式。

活动现场学生们积极参与有奖问答活动，与网络举报辟谣的 IP 形象“豹豹”人偶打卡合影、并在宣传横幅上留下了签名，立志做网络信息安全的践行者、引导者和捍卫者。

通过本次网络举报校园宣传活动，进一步提升了全校学生的网络安全意识，有助于引导广大学生做到不造谣、不信谣、不传谣，发现网上违法和不良信息积极举报，自觉成为网络文明建设的践行者和传播者，共同参与到网络综合治理中来，从而营造清朗的校园网络环境。

（信息来源：https://net.xju.edu.cn/info/1046/1420.htm）

二．福州大学举办 2023 年网络安全宣传周专题讲座

2023 年 9 月 14 日上午，福州大学 2023 年网络安全宣传周专题讲座在旗山校区图书馆博学厅举行，邀请网络安全行业专家曾煜、计算机与大数据学院董晨副教授进行交流分享。讲座由学生工作部（处）、网络安全与信息化办公室主办，计算机与大数据学院承办，近 400 名学生参加培训。

网络安全专家曾煜从网络安全法律法规、校园网络安全态势以及攻防演练所暴露出的典型问题出发，结合实际案例，介绍个人信息安全、邮件安全、数据安全等网络安全知识。计算机与大数据学院董晨副教授从大数据安全、人工智能安全、区块链安全、集成电路安全、生物芯片安全等方面介绍网络安全学科前沿研究，并重点介绍我校网络安全学科研究情况。

此次安全周，除了专题讲座外，学校还制作了宣传手册向在校学生发放，张贴各类宣传海报进行宣传，开展了网络安全知识小程序答题活动，充分营造“网络安全为人民、网络安全靠人民”的网络安全宣传周氛围，进一步提升学生的网络安全防范技能，强化网络安全风险防范意识，拓宽学生对网络安全学科的认识。

（信息来源：https://wxb.fzu.edu.cn/info/1007/1941.htm）

策划：李向龙　　摘编：刘玉燕　　微信发布：张丽丽　网站发布：郭思佳