DOI：10. 3969/j. issn. 2096-045X. 2026. 01. 020

·院校管理·

高校电子邮件系统安全防护体系构建与实践
——以首都医科大学为例

董秀蕾　赵志强*
（首都医科大学信息化处，北京 100069）

【摘要】电子邮件服务是一种广泛使用的互联网服务，是校园网重要基础服务之一。电子邮件为学校师生工作学习带来了便利，然而在网络安全防护中却成为主要攻击目标。在大国博弈中网络空间安全越发严峻的背景下，电子邮件系统的安全运维和管理成为校园网信息安全防护的重点。本文通过分析当前电子邮件安全形势，从整体安全技术架构体系、使用安全扩展协议、强化信息与账号防护、邮件网关安全防护和提升用户安全防范意识等多个角度阐述应对电子邮件安全风险的措施，对提升学校信息安全具有重要意义。

【关键词】电子邮件；信息安全；风险分析；防护；网络安全；邮件网关
【中图分类号】TP393　　【文献标识码】A

Construction and practice of security protection system for university email systems —a case study of Capital Medical University

Dong XiuLei, Zhao ZhiQiang*
(*Information Technology Department, Capital Medical University, Beijing 100069, China*)

【**Abstract**】Email service, a prevalent internet service, stands as one of the indispensable system services within campus networks. Email communication offers convenience in daily work and academic pursuits. However, it has also emerged as a primary target for cyberattacks. Amid the increasingly grave challenges in cybersecurity, the secure operation and maintenance of email systems and the safety management of communications have become crucial focal points in information security protection for campus networks. This paper conducts an analysis of the current email security situation and puts forward countermeasures against email security risks from multiple perspectives, including the establishment of a comprehensive security technology architecture system, the implementation of secure extension protocols, the reinforcement of information security and account protection, the enhancement of email gateway security, and the improvement of user security awareness. These measures play a crucial role in advancing information security on campus environments.

【**Keywords**】email; information security; risk analysis; defense; cybersecurity; mail gateway

雷·汤姆林森1971年发明了电子邮件[1]，20世纪80年代我国第一封电子邮件发出后[2]，电子邮件被快速应用到各个领域。电子邮件被广泛使用的同时也承载了众多领域重要且敏感的信息，因此成为黑客关注的重点目标。电子邮件的安全关系到校园网络安全、社会秩序、公共利益，甚至国家安全。本文旨在研究探讨高校电子邮件系统面临的典型安全风险，构建适应高校特点的多层次防护体系，并提出优化的管理策略。

第一作者　董秀蕾，硕士，高级工程师，研究方向：高校信息化。Email：dongxl@ccmu.edu.cn
*通信作者　赵志强，博士，研究员，首都医科大学信息化处处长，研究方向：医科教育、高校信息化。Email：zzq@ccmu.edu.cn

1 电子邮件安全形势分析

1.1 网络安全事件回顾

近年来,暴露的网络安全事件多与电子邮件相关。2018年3月,美国司法部发布起诉书指出,伊朗黑客针对数百家美国和国外大学以及数十家美国公司和政府机构发动网络攻击,盗取了价值高达34亿美元的31 TB数据资料和知识产权。这些黑客冒充其他大学的教授向受害者发送钓鱼邮件,声称对他们的研究成果感兴趣,用户点击邮件中虚假网站的链接后,弹出的网页使用户难以鉴别是否为真实系统,引诱受害者重新输入用户名密码,个人资料被轻松窃取[3]。2022年4月,某校发布声明称遭受境外网络攻击,学校师生收到来自黑客组织和不法分子发送的钓鱼邮件,主要涉及科研评审、答辩邀请和出国通知等。邮件内容引诱师生点击伪装链接,非法获取师生电子邮箱账号密码,并企图窃取相关师生邮件数据和个人信息。同时,邮件中的木马程序以隐蔽手段获取运行权限。经过技术分析与溯源,该校的信息网络中发现了多款源于境外的木马样本,该校网络和运维的关键核心技术数据被窃取,对学校信息系统和广大师生的重要数据造成重大安全威胁[4-5]。

1.2 校园网和电子邮件安全风险分析

网络安全事件层出不穷,国家相继出台《中华人民共和国网络安全法》和网络安全等级保护基本要求2.0[6](以下简称等保2.0)等法律法规和标准,严防死守网络安全底线。为了加强网络安全防护意识,提升关键信息基础设施和重要信息系统防护水平,国家全面开展护网专项行动。护网行动是国家应对网络安全问题所做的重要布局之一,所有单位有序完成护网行动是必不可少和必须做扎实的一项基础工作。面对复杂严峻的网络安全形势,国家大力推动邮件安全发展[7],要求系统部署、综合施策,加强电子邮件系统的安全防护。

2022年7月,某校电子邮件用户因安全意识较差,将账号名作为了密码的一部分,生活邮箱与工作邮箱混用,导致其邮箱账号被成功窃取。攻击队通过第三方网站获取了用户基本信息和工作单位后,通过爬虫官方网站获取到该用户电子邮箱地址,使用社工库拿到用户的历史密码并生成密码字典,后经过多次登录尝试后窃取到用户邮箱密码。电子邮件是网络攻击的主要途径之一,常常是校园网安全的第一道防线,加强电子邮件系统的安全防护是校园网整体安全防护的关键环节。

2 电子邮件系统安全防护体系构建

2.1 研究方法

本文通过网络层次化安全体系分析,将电子邮件系统安全防护划分为协议层、数据层、应用层、用户层,各层级防护与校园网整体防御体系系统联动,构建完整邮件安全防护架构。安全扩展协议解决传输过程的身份验证与防篡改。数据加密存储和传输保障全生命周期的数据安全。用户登录多因素验证和安全宣传弥补人为因素漏洞。通过增加垃圾邮件专用检测设备抵御应用层恶意流量,提升检测效率和降低邮件系统的维护成本。

2.2 校园网整体防护基础

校园网整体安全布局是邮件安全风险防护的基石,邮件安全风险的应对依托于校园网整体网络安全的管理技术体系。电子邮件系统应运行在可靠的物理和网络环境中,防止物理篡改。校园网应具备配套的管理规章制度和专人负责安全运维,建立可执行的突发网络安全事件应急响应预案。

电子邮件安全管理和技术体系是邮件安全风险应对的核心[8]。系统在建设前应按照等保2.0的要求进行定级,并按照定级标准建设和修正系统。按照系统安全技术要求加强电子邮件系统的安全管控,对关键数据进行加密存储和传输,加强身份鉴别等安全措施,降低数据被窃取的风险。规范系统安全运行的要求和管理措施,

构建完整防御体系[9]。根据需要对系统和软件不定期进行漏洞扫描和渗透测试,积极整改已发现的安全漏洞和不定期升级等,增强系统的健壮性。

2.3 使用安全扩展协议

电子邮件传输协议最初设计时安全性考虑不足,简单邮件传输协议(simple mail transfer protocol,SMTP)主要用于系统之间的邮件信息传递,但存在明文传输和认证机制薄弱,未考虑到防止冒充和欺骗等安全性问题。黑客可利用漏洞人为构造发件人等参数修改邮件头信息,甚至搭建私人服务器制造并发送虚假邮件。为了弥补早期SMTP的安全性缺陷,业界相继增加优化了一些针对电子邮件身份验证扩展协议,试图解决发件人伪造攻击,辅助SMTP加强电子邮件安全[10],用于防伪造机制和反垃圾邮件。电子邮件系统应积极配置发信者策略架构(sender policy framework,SPF)协议、域名秘钥识别邮件标准(domain keys identified mail,DKIM)协议和基于域的邮件验证报告和一致性(domain-based message authentication, reporting and conformance, DMARC)协议这3个扩展协议,并验证配置的正确性来强化电子邮件系统安全。

2.3.1 发信者策略架构协议

SPF可以确保电子邮件来源的真实性,防止攻击者仿冒发件人身份进行网络钓鱼攻击。SPF协议是一种DNS(domain name system)记录类型,标识发信域名的真实IP地址。收信方判断发件人经过的SMTP服务器是否来自发送域指定的IP地址,即邮件是否由合法邮件服务器发出。

2.3.2 域名秘钥识别邮件标准协议

DKIM基于传统的密钥认证方式,公钥存放在DNS用来验证签名,私钥存放在发信服务器中用来签署域名。用户发送邮件时,发信服务器将加密签名插入到出站的电子邮件的邮件头中,将该签名与域名关联。收信服务器使用公钥验证邮件签名,从而判定电子邮件及发送方信息的真实性,若不一致则为垃圾邮件,保障邮件内容不被偷窥或篡改。

2.3.3 基于域的邮件验证报告和一致性协议

DMARC协议是基于SPF和DKIM协议发展而来的电子邮件身份认证协议,由收发双方提供邮件反馈机制。接收方获取DMARC记录,对邮件进行SPF和DKIM验证,验证失败的邮件根据DMARC记录进行处理,并反馈给发送方。同时添加了域名对齐检查和报告发送功能,声明如何处理验证失败的邮件[11]。DMARC协议综合了SPF和DKIM协议的检测结果,验证发件人身份的真实性,以及邮件内容是否被篡改;同时将验证失败的邮件信息根据DMARC记录进行处理后反馈给发送方做进一步审查[12]。使用这些协议可在很大程度上过滤非法发送的垃圾邮件。

2.4 数据加密存储和传输

在数据存储上对用户数据尤其是关键数据进行加密存储,并使用国家密码管理局认可的加密手段。为了保障传输数据安全,使用加密方式传输密码和邮件内容,系统应支持基于安全套接层(secure socket layer, SSL)端到端的安全数据传输通信协议。SSL为互联网的各种协议给与支持,使用SSL的业务可以做到客户端和服务器的双向认证,在通信的握手过程中建立密钥和算法加密,以防止通过使用IP数据包嗅探工具非法窃听。

邮件系统支持包括超文本传输协议(hypertext transfer protocol secure, HTTPS)和加密版本的SMTPS、POP3S、IMAP4S等协议进行安全数据传输,他们是SMTP、POP3(post office protocol-version 3)和IMAP(internet mail access protocol)协议基于SSL安全协议之上的变种协议,继承了SSL安全协议的非对称加密的高度安全可靠性,可以实现登录以及整个邮件会话的安全加密,防止邮件泄露、被黑客截取数据,还可实现邮件发送者抗抵赖功能[13]。用户访问webmail时系统强制转换HTTPS保障邮件数据加密传输。在使用邮件客户端访问系统时,为了不破坏用户使用习惯,首先从鼓励用户邮件客户端配置安全端口开始,到逐步全面启用SSL安全端口,最终关闭系统的非安全端口,实现传输全

链路加密。

2.5 阻断垃圾邮件

2.5.1 邮件系统内置过滤机制

垃圾邮件的过滤对电子邮件系统非常重要，通常邮件系统同时配备反垃圾邮件和反病毒引擎。日常垃圾邮件的处理措施通常包括：阻断恶意IP、锁定被盗邮箱、建立黑名单等。通过校企间合作主动发现、主动防御，阻断已被发现的恶意IP。也可以借助开源软件分析日志，编写脚本有针对性地阻断暴力破解账号的恶意IP等。但过滤设置过于严苛会导致正常邮件接收困难，应权衡利弊，灵活配置，保证正常接收的同时尽可能地限制垃圾邮件。

2.5.2 防止盗号被黑客利用

被盗账号一般会被攻击者利用发送垃圾邮件。邮件系统可通过系统内置保护措施，编写补充脚本等技术手段，结合人工分析监控用户发送邮件情况，及时采取措施封禁危险账号。邮件系统需要为用户提供友好界面的通知和提醒，如陌生人邮件提醒、邮件中不安全链接弹窗提醒等，可以帮助用户更好地判断邮件的真实性，降低被盗风险，避免被利用发送垃圾邮件；同时鼓励用户举报漏判的垃圾邮件，增加过滤样本丰富性。

2.6 邮件网关安全防护

2.6.1 钓鱼邮件威胁趋势升级

在不断升级的网络安全威胁中，面临越来越多的钓鱼欺诈邮件、勒索邮件等安全威胁，钓鱼攻击已成为黑客频繁采用的手段。很多网络安全事件的起因是用户被成功钓鱼后，打开了网络安全防护的缺口，从而造成更大损失。由于租用云服务器和注册域名的便捷和低廉性，使得攻击者可以用很低的成本轻易构建邮件攻击框架。当前不法分子具有较强的反侦察意识，为了绕过检测设备，他们精细化管理，为服务器配置SPF、DKIM以假乱真，生成大量随机域名做跳板，使用域名调度，最终指向真实资产IP，目的是保证其网站存活性。

国内各行业遭受垃圾邮件侵扰分布多有变化，文献[14]中提及的《2023年第三季度企业邮箱安全报告》指出，国内各行业接收垃圾邮件的域名列表TOP100中，凸显教育行业遭受垃圾邮件攻击十分严重，成为垃圾邮件的重灾区，教育行业需特别引起重视。结合历年分析报告，电子邮件使用规模与使用频次持续上升，与之相伴的钓鱼邮件数量大幅增长[15]。

2.6.2 增加邮件网关过滤所有投递邮件

单一的防护策略有其弊端，设置IP黑名单有可能拒收正常邮件。对于突发大量垃圾邮件，可以采取关键字过滤，但通过设置关键字也增加了误拦截的概率，邮件主题越短越容易造成误拦截。为了更好地抵御垃圾邮件攻击，加强技术手段防范钓鱼邮件非常重要。在邮件系统前端增加专业检测过滤设备，依赖深度学习的实时大数据分析的邮件网关可作为SMTP网关、反垃圾和反病毒引擎，与邮件系统协同工作，组成深度防护体系过滤恶意邮件，所有来信进入邮件系统前检测过滤，高风险邮件进入隔离区（图1）。

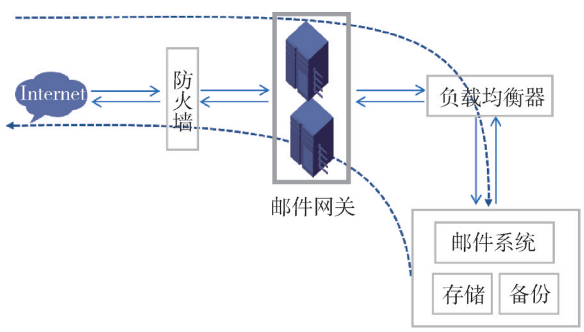

图1 邮件网关和邮件系统拓扑图

使用邮件网关后需要调整邮件系统相关配置，如关闭实时黑名单（real-time blacklist，RBL）检查，由邮件网关进行RBL检查、SPF策略检查、域名检测、IP过滤、内容特征检测等技术的多种方法综合研判，可避免因RBL检测启用邮件系统的重投机制或者退信，造成系统和网络资源过度消耗。邮件网关能够抵御高频邮件攻击，减轻邮件服务器的压力，隔离病毒和恶意邮件。另外，应重点关注攻击者向被盗账户通讯录中联系人，以及本系统内其他用户发送恶意邮件的横向钓鱼攻击。这些钓鱼邮件来自已知的、受信任的真实账户，不仅占用网络和系统资源，更重要的

是直接利用了人们的信任关系，邮件内容可能与正常工作交流非常相似，更加难以检测。用户接收和发送的邮件都经过邮件网关研判后再投递给收件人，在一定程度上能够拦截特征相对明显的钓鱼邮件。

当前研究发现，黑客对基础网络架构的攻击时间不断缩短，网络钓鱼邮件的攻击也存在同样的趋势。从2022年第四季度开始，为规避传统邮件防护机制，攻击者经过充分研究和精心设计的针对性攻击，正在取代无差别的大规模邮件攻击活动。这些邮件使用伪造身份、更加隐蔽的标题、附带恶意程序的附件等多种手段。攻击者制造发送的社会工程学精准钓鱼邮件具有少量、低频次投递特点，与正常邮件无异，有更高转化率和成功率，使得识别威胁和攻击溯源等安全防范工作更加困难[16]。

2.7　强化信息安全与账号防护

2.7.1　Webmail身份认证安全机制

从前述安全形势分析中发现，电子邮件攻击多由人本身作为突破点，提升用户层安全防护是安全防范的关键。弱用户口令很容易被暴力破解，强口令能够提供身份鉴别的安全关键，防止账号泄露后成为发送钓鱼邮件的跳板。由于黑客产业化发展，邮箱账号经常被暴力破解，账号被盗事件时有发生，单因素认证已经无法满足安全性需求。开启多因素身份验证机制被提上日程，即webmail登录不再依赖单一密码验证，而是密码加动态验证码的双重验证来提供更加安全的登录方式。

2.7.2　邮件客户端使用专用密码

用户除了使用webmail访问邮箱以外，大量用户仍会使用电子邮件客户端。与其他信息系统比较，用户侧使用的电子邮件客户端既是数据源，又是数据终端，同时传输和存储用户数据，因此增加用户侧的安全性显得尤为重要。为了防止客户端成为泄密途径，提醒用户使用安全客户端软件，并加强客户端身份校验[17]。将webmail的身份验证与客户端的验证分开，客户端使用随机生成且不可复制的复杂专用密码。除此之外，还要设置用户账号多次登录失败的处理机制，协同抵抗暴力破解。基于动态IP池的账号爆破方式，使得很多传统的防爆破技术失效。使用多因素身份验证，同时客户端使用专用密码可大大降低账号被盗风险。

2.7.3　提升用户安全意识

电子邮件系统的信息安全问题，离不开用户的安全防范意识。用户作为安全生态系统中的主动参与者对于电子邮件的安全防范至关重要。当前攻击者依托电子邮件利用社会工程学技巧发起网络攻击已经是常见的攻击方法[18]。用户通常被认为是整个防御系统中最脆弱的一个环节，因此不断加强用户安全意识在防范钓鱼邮件攻击中具有非常重要的意义。系统层面可通过多种技术手段加强用户信息安全。而用户更应高度警惕，自主保护个人信息和账号不被窃取。如避免多系统共用密码导致交叉泄露风险；不在第三方网站随意留下个人信息；不在咖啡厅、机场等公共Wi-Fi环境中访问邮箱；不被钓鱼邮件的主题和内容左右，不轻易点击邮件中的链接和附件，以及扫描正文中的二维码等。这些良好的行为习惯都是保护个人账号安全的有效方法。信息安全部门需要通过多种方式广泛宣传，督促全体用户提升网络和电子邮件安全防范意识。

通过多层次构建电子邮件防护体系，提升钓鱼邮件等恶意邮件的拦截率。系统全员开启多因素验证前经常发生邮箱被盗，开启多因素认证同时启用客户端专用密码后未发生账号被盗。通过安全扩展协议等方式实现传输和存储的全链路加密，有效防止数据在传输过程中被窃取或篡改。在防范威胁、保障数据资产和控制风险成本等方面取得显著成效。

3　结　语

电子邮件信息安全是校园网整体安全的核心要素之一，做好安全防范应从技术和管理两个方面开展。监管部门和云平台提供方需加强网络安全管理，有效落实主体责任，不给不法分子可乘之机。学校要采用符合安全标准的产品，产品提供方有义务配合学校及时修补漏洞，协助更

新迭代产品,提升系统健壮性。管理人员要紧跟时事,对安全事态进行研判,采取合理的主动措施将风险降到最低,并积极参与高校和企业间的安全合作,共享威胁情报,及时交流最新的邮件安全策略和防御技巧,共同提高电子邮件的安全防护水平。学校定期开展师生网络安全培训,鼓励用户通过系统主动举报潜在威胁邮件。在条件允许的情况下增加专用垃圾邮件过滤检测设备。随着人工智能技术的不断发展,电子邮件攻防对抗将进一步加剧,邮件攻防双方已向智能化和精准化演变,依托人工智能技术加持,邮件安全防护的策略和技术能力将进一步加强。

利益冲突 所有作者声明不存在利益冲突。

作者贡献声明 董秀蕾:项目设计,部署实施,方案修正,撰写、修订论文;赵志强:论文指导和审定。

参考文献

[1] 李忠东. 电子邮件中的@[J]. 铁道知识,2005(1):13.

[2] 吴为民. 中国第一封电子邮件[J]. 现代物理知识,2009,21(3):57-61.

[3] 杨海明. 浅析电子邮件的安全[J]. 办公自动化,2022,27(8):53-55.

[4] 国家计算机病毒应急处理中心 计算机病毒防治产品检验中心. 西北工业大学遭美国NSA网络攻击事件调查报告(之一)[EB/OL]. (2022-09-05)[2025-03-01]. https://www. cverc. org. cn/head/zhaiyao/news20220905-NPU. htm.

[5] 国家计算机病毒应急处理中心 计算机病毒防治产品检验中心. 西北工业大学遭美国NSA网络攻击事件调查报告(之二)[EB/OL]. (2022-09-27)[2025-03-01]. https://www. cverc. org. cn/head/zhaiyao/news20220927-NPU2. htm.

[6] 全国信息安全标准化技术委员会(SAC/TC 260). 信息安全技术 网络安全等级保护基本要求:GB/T 22239-2019[S]. 北京:中国标准出版社,2019.

[7] 袁硕. 博物馆邮件系统安全浅析[J]. 中国建设信息化,2018(1):70-71.

[8] 李文婷,张格,刘冬. 电子邮件网络安全风险分析及应对[J]. 保密科学技术,2021(9):69-71.

[9] 梁利,蔡先勇,李文杰,等. 电子邮件系统安全技术要求标准应用[J]. 信息技术与标准化,2022(5):76-78.

[10] 崔宁,薛质,施勇,等. 基于SPF和DMARC协议应用分析的邮件安全形势研究[J]. 通信技术,2021,54(12):2703-2710.

[11] 袁静怡,李子川,彭国军. EN-Bypass:针对邮件代发提醒机制的安全评估方法[J]. 网络与信息安全学报,2023,9(3):90-101.

[12] 尚菁菁,朱宇佳,刘庆云. 电子邮件安全扩展协议应用分析[J]. 网络与信息安全学报,2020,6(6):69-79.

[13] 樊华,甘杰夫,寇春晓,等. 政府部门邮件系统安全现状研究[J]. 信息安全与通信保密,2016(9):55-58,62.

[14] 邮箱网. 2023年Q3企业邮箱安全性报告:境内钓鱼邮件超过境外攻击[EB/OL]. (2023-10-31)[2025-03-01]. http://www. chinaemail. com. cn/blog/content/14458/.

[15] CACTER邮件安全. 2024年中国企业邮箱安全性研究报告:揭秘恶意邮件神秘幕后推手[EB/OL]. (2025-03-31)[2025-04-02]. https://www. freebuf. com/articles/paper/426181. html.

[16] 张如旭. 2021电子邮件安全的五大趋势[J]. 计算机与网络,2021,47(1):52-53.

[17] 蒲小英,付敏. 电子邮件系统安全特性及防护方向[J]. 电脑知识与技术,2019,15(28):38-39.

[18] 梁宏,张慧云,肖新光. 基于社会工程学的邮件样本关联分析[J]. 信息网络安全,2015,15(9):180-185.

(收稿日期:2025-04-09,修回日期:2025-05-15)
(本文编辑:高健)

开放获取 本文使用遵循知识共享 署名-非商业性-禁止演绎4.0协议(CC BY-NC-ND 4.0),详细信息请访问 https://creativecommons. org/licenses/by-nc-nd/4.0/。

OPEN ACCESS This article is licensed for use under Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Deed (CC BY-NC-ND 4.0). For more information, visit https://creativecommons.org/licenses/by-nc-nd/4.0/.