基于信息技术的网络安全漏洞监测与防范策略研究

■ 谷 雨

【摘要】随着信息技术的迅猛发展，网络全方位融入社会生活的各个层面。网络安全漏洞作为网络安全的核心议题之一，给个人隐私、企业运营以及国家信息安全带来了极大的威胁。本文深度剖析基于信息技术的网络安全漏洞监测与防范策略。先阐述网络安全漏洞的概念、分类及危害，接着全面分析当下的监测技术与防范策略，致力于提升医院网络系统的安全性与稳定性，确保信息的安全传输与存储。

【关键词】信息技术；网络安全漏洞；监测技术；防范策略

DOI：10.20167/j.cnki.ISSN1673-7911.2025.06.21

0 引言

在当今信息时代，网络已然成为信息传递、资源共享以及业务开展的关键平台。从日常生活中的移动支付、社交互动，到企业的线上办公、电商交易，到医疗机构的远程会诊、互联网医院，再到政府部门的电子政务，网络无处不在。由于网络安全漏洞的频繁出现，使得网络安全形势愈发严峻。网络安全漏洞是指在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，这些缺陷为攻击者提供了可乘之机，可能引发系统瘫痪、数据泄露、隐私侵犯等严重后果，给用户带来难以估量的损失。2017 年的 WannaCry 勒索病毒事件，该病毒利用 Windows 系统的 SMB 漏洞进行大规模传播，短时间内席卷全球，感染了大量计算机，众多企业和机构的业务被迫中断，文件被加密勒索，造成了巨大的经济损失和恶劣的社会影响。据统计，此次事件波及 150 多个国家和地区，直接经济损失达数十亿美元。这一事件为全球网络安全敲响了警钟，凸显了加强网络安全漏洞监测与防范的紧迫性和重要性 [1]。网络安全漏洞不仅威胁到个人的隐私和财产安全，也对医疗机构的正常运营和可持续发展构成挑战。对于医疗机构而言，信息数据是核心资产，一旦发生数据泄露事件，不仅会损害医疗机构的声誉，还可能面临患者隐私的泄露和法律诉讼的风险。而对于医院层面，网络安全关乎医院诊疗业务的正常开展，关键信息基础设施若遭受攻击，可能引发社会公共事件，危及医院正常运营。对网络安全漏洞监测与防范策略进行深入探讨，具有极其重要的现实意义和战略价值。

1 网络安全漏洞概述

1.1 网络安全漏洞的定义

网络安全漏洞指的是在硬件、软件、协议的具体实现过程中，或是系统安全策略方面存在的缺陷，攻击者可借此在未经授权的情况下访问或破坏系统。这些漏洞的产生原因复杂多样，可能源于程序设计过程中的疏忽、逻辑错误，也可能是系统配置不当、安全策略不完善等因素所致。

1.2 网络安全漏洞的危害

（1）信息泄露：攻击者利用网络安全漏洞，能够获取系统中的敏感信息，如个人隐私数据、企业商业机密、政府机密文件等。这些信息一旦泄露，不仅会损害个人权益，还可能对企业的竞争力和国家的安全造成严重威胁。2018 年万豪酒店数据泄露事件，约 5 亿客户信息被泄露，涉及客户姓名、地址、电话号码、护照号码等敏感信息，给客户带来了极大的困扰，同时也使万豪酒店的声誉遭受重创，使其面临巨额赔偿和客户流失的风险。

（2）系统瘫痪：通过利用漏洞发动拒绝服务攻击（DoS 或 DDoS），攻击者可使目标系统瘫痪，无法正常提供服务。针对网站的 DDoS 攻击，攻击者通过控制大量的傀儡机，向网站服务器发送海量的请求，耗尽服务器的资源，导致网站无法访问。这对于依赖网站进行业务开展的企业来说，可能意味着业务中断，经济损失惨重。据统计，一次大规模的 DDoS 攻击可能导致企业每小时损失数十万元甚至更多。

（3）数据篡改：攻击者利用漏洞修改系统中的数据，如篡改财务数据、篡改诊疗记录等，这将破坏数据的完整性和真实性。对于企业而言，数据的准确性至关重要，篡改后的财务数据可能导致企业决策失误，财务报表失真，影响企业的融资和发展。在医疗领域，诊疗记录的篡改可能引发业务风险，损害患者利益 [2]。

（4）恶意控制：黑客利用漏洞获取系统的控制权后，

中国知网 https://www.cnki.net

会在系统中植入恶意软件，如木马、病毒等，进而对系统进行远程控制。他们可以利用被控制的系统进行进一步的攻击，如发动 DDoS 攻击、窃取更多的信息等。一些僵尸网络就是通过控制大量被植入木马的计算机，进行各种恶意活动，严重危害网络安全。

2 网络安全漏洞监测技术

2.1 基于特征匹配的监测技术

（1）工作原理：基于特征匹配的监测技术通过提取已知漏洞的特征信息，如漏洞的代码模式、攻击行为特征等，构建特征库。在监测过程中，系统实时采集网络数据，并将其与特征库中的特征进行比对。一旦发现匹配项，便判定存在相应的安全漏洞。以入侵检测系统（IDS）为例，它利用特征匹配技术来检测已知的攻击行为。当网络流量中出现与特征库中记录的攻击特征一致的流量时，IDS 就会发出警报。

（2）优点：检测准确率较高，对于已知漏洞的检测效果显著。只要特征库足够完善，就能准确地识别出已知的攻击和漏洞，误报率相对较低。并且该技术成熟度高，经过长期的发展和应用，已经广泛应用于各种安全产品中，为网络安全防护提供了有力支持。

（3）缺点：无法检测新出现的未知漏洞，因为它完全依赖于已知漏洞的特征库。对于新型的攻击手段和未知漏洞，由于缺乏相应的特征信息，系统无法做出有效的检测。而且特征库的维护成本较高，随着网络攻击手段的不断更新和变化，需要持续投入大量的人力和时间来收集、分析和更新特征库，以确保其能够适应新的安全威胁 [3]。

2.2 基于异常检测的监测技术

（1）工作原理：异常检测技术通过建立系统或用户的正常行为模型，该模型基于对系统或用户在正常状态下的行为数据进行分析和学习而得到。当监测到的行为与正常模型出现显著偏离时，系统就认为可能存在安全漏洞或攻击行为。通过监测网络流量的异常波动、用户登录行为的异常模式等来发现潜在的安全问题。如果某个用户在短时间内从多个不同的 IP 地址登录系统，且登录频率远超正常水平，就可能被判定为异常登录行为，系统会发出警报。

（2）优点：能够检测未知漏洞和新型攻击，具有较强的自适应性。它不依赖于已知的攻击特征，而是通过对行为模式的分析来发现异常，从而对于新出现的攻击手段和未知漏洞有一定的检测能力。并且可以根据不同的网络环境和系统特点，自动学习和调整正常行为模型，适应能力较强 [3]。

（3）缺点：误报率较高，由于正常行为的定义存在一定的模糊性，一些正常的行为变化可能也会被误判为异常。医院在进行大规模的数据备份或系统升级时，网络流量和系统资源使用情况可能会出现较大波动，容易被误报为攻击行为，这增加了安全管理人员的工作量和判断难度。而且模型建立复杂，需要对大量的历史数据进行深入分析和处理，并且要不断地进行优化和调整，以提高模型的准确性和可靠性，技术难度较大。

2.3 基于漏洞扫描的监测技术

（1）工作原理：漏洞扫描技术利用专门的扫描工具对网络系统、服务器、应用程序等进行全面检测，查找其中存在的安全漏洞。扫描工具通常会依据预先定义的漏洞规则库，对目标系统进行多种测试，如端口扫描、服务检测、弱口令检测等。端口扫描用于发现目标系统开放的端口，不同的端口对应不同的服务，通过分析开放的端口，可以了解系统提供的服务类型，进而判断是否存在安全风险。服务检测则是检查系统中运行的服务是否存在已知的漏洞。弱口令检测用于发现用户设置的简单易猜的密码。根据扫描结果，生成详细的漏洞报告，报告中会指出系统中存在的漏洞类型、位置和严重程度等信息。常见的漏洞扫描工具有 Nessus、OpenVAS 等。

（2）优点：能够快速、全面地发现系统中的已知漏洞，为后续的漏洞修复提供有力依据。通过定期进行漏洞扫描，可以及时发现信息系统中新增的漏洞，便于及时采取防范措施。而且扫描工具操作相对简单，即使是非专业的安全人员也能在一定程度上使用，有助于普及网络安全检测工作 [4]。

（3）缺点：对一些复杂的、需要深入分析的漏洞可能检测不到，因为扫描工具主要依据预先定义的规则库进行检测，对于一些新型的、尚未被收录到规则库中的复杂漏洞，可能无法有效识别。扫描过程可能会对目标系统的性能产生一定影响，大规模的漏洞扫描可能会占用目标系统的大量资源，导致系统运行缓慢，甚至在扫描一些性能较低的设备时，可能会引发系统短暂瘫痪。

2.4 基于机器学习的监测技术

（1）工作原理：机器学习技术在网络安全漏洞监测领域的应用日益广泛。通过对大量的网络安全数据进行学习和训练，建立机器学习模型，让模型自动识别网络数据中的安全模式和异常行为。利用深度学习算法对网络流量数据进行分析，识别其中的恶意流量。深度学习算法可以自动提取数据中的复杂特征，从而更准确地判

中国知网 https://www.cnki.net

断流量是否为恶意。使用聚类算法对用户行为数据进行聚类，发现异常用户行为。聚类算法可以将相似的用户行为归为一类，当出现与其他类差异较大的行为时，就可能被判定为异常行为。

（2）优点：能够不断学习和适应新的安全威胁，随着学习数据的不断增加，模型的检测性能会不断提高。对于复杂的网络数据和新型的攻击手段，机器学习技术具有较强的处理能力，能够发现传统监测技术难以察觉的安全隐患，提高漏洞监测的准确性和效率。

（3）缺点：需要大量的高质量数据进行训练，数据的质量直接影响模型的性能。如果数据存在问题，会导致模型的准确性和可靠性下降。模型的训练和维护成本较高，需要专业的技术人员和强大的计算资源来进行模型的训练、优化和更新。而且模型的可解释性较差，对于一些复杂的机器学习模型，如深度学习模型，其决策过程难以直观解释，安全管理人员难以理解模型为什么做出这样的判断，增加了使用和维护的难度。

3 网络安全漏洞防范策略

3.1 安全补丁管理

及时安装软件供应商发布的安全补丁是防范网络安全漏洞的重要措施。软件供应商会定期修复已知的安全漏洞，并发布相应的补丁程序。用户和企业应建立完善的补丁管理机制，及时获取并安装补丁。首先，要建立补丁信息收集渠道，关注软件供应商的官方网站、安全公告等，及时了解补丁发布信息；其次，制定合理的补丁测试和部署计划，在安装补丁前，先在测试环境中进行充分测试，确保补丁不会对系统的正常运行产生负面影响，然后再逐步推广到生产环境；最后，加强对补丁安装情况的监控和管理，定期检查系统是否已安装最新的安全补丁，对于未安装补丁的系统及时进行提醒和处理。

3.2 访问控制策略

实施严格的访问控制策略可以有效限制非法用户对系统资源的访问，降低安全漏洞被利用的风险。访问控制策略主要包括用户身份认证、授权和访问权限管理。用户身份认证是确认用户身份的过程，常见的认证方式有用户名 / 密码认证、指纹识别、智能卡认证等。通过多种认证方式的结合，可以提高认证的安全性。授权是根据用户的身份和角色，赋予其相应的访问权限。企业应根据业务需求，合理划分用户角色，并为每个角色分配最小化的访问权限，遵循“最小权限原则”。普通员工只赋予其访问与工作相关的文件和应用程序的权限，而系统管理员则拥有更高的权限，但也应受到严格的监督和管理。此外，还要定期对用户的访问权限进行审查和更新，确保权限的分配始终符合用户的实际工作需求。

3.3 网络安全隔离

网络安全隔离是将不同安全级别的网络或系统进行隔离，防止安全漏洞在不同区域之间传播。常见的网络安全隔离技术有防火墙、虚拟专用网络（VPN）和网闸等。企业应根据自身的网络架构和安全需求，合理部署网络安全隔离设备，构建多层次的网络安全防护体系。

3.4 安全意识培训

提高员工的安全意识是防范网络安全漏洞事件的基础。许多安全漏洞事件的产生是由于员工安全意识不足，如点击恶意链接、使用弱密码、随意共享敏感信息等。医院应加强对员工的安全意识培训，定期开展安全知识讲座、培训课程和模拟演练等活动。培训内容包括网络安全基础知识、安全操作规范、常见安全威胁及防范措施等。通过提高员工的安全意识，使其了解网络安全的重要性，掌握基本的安全防范技能，从而减少因人为因素导致的安全事件。

4 结语

网络安全漏洞的监测与防范是保障网络安全的关键环节。本文通过对网络安全漏洞监测技术和防范策略的研究，分析了当前存在的问题，并提出了相应的改进建议和未来发展方向。在信息技术不断发展的背景下，网络安全面临着日益复杂的挑战，我们需要不断创新和完善网络安全漏洞监测与防范技术和策略，加强各方面的协同合作，提高网络安全防护能力，保障网络空间的安全与稳定。只有这样，才能适应时代发展的需求，保护个人、企业和国家的信息安全。

参考文献

[1] 强立新，何炎．浅析计算机网络安全防范措施 [J]. 价值工程，2015(07):69-70.

[2] 张忠东，胡利娜，宋慧艳，等．计算机信息管理在网络安全中的应用 [J]. 中小企业管理与科技，2015(04):310-311.

[3] 聂丽伟．计算机网络安全现状及常用解决方案 [J]. 计算机与网络，2015(02):51.

[4] 王亚飞．模糊层次分析法在计算机网络安全评价中的运用 [J]. 价值工程，2015(06):247-248.

作者简介：谷雨（1979-），男，本科，工程师，研究方向：网络信息安全。

（作者单位：安徽医科大学第一附属医院）

中国知网 https://www.cnki.net