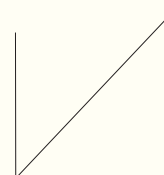


信息化建设中网络安全与维护策略探究

文◆大庆油田数智技术公司 张明

引言

网络安全与维护在信息化建设中扮演着至关重要的角色，它不仅关乎企业和组织信息系统的运行稳定性、数据安全性以及业务连续性，还关系到企业和用户的利益保护和社会稳定发展。因此，加强网络安全与维护工作，提高对网络安全重要性的认识，制定科学合理的安全策略，实施有效的安全措施，是信息化建设中不可或缺的重要环节。



1 网络安全与维护在信息化建设中的关键作用

1.1 保障信息化系统正常运行

网络安全与维护在信息化建设中的关键作用之一是保障信息化系统正常运行。随着信息化程度的不断提高，企业和组织的各项活动都离不开网络系统的支持。如果网络受到攻击或遭遇故障，那么会导致系统瘫痪、数据丢失甚至机密信息泄露等严重后果。建立完善的网络安全策略和维护机制，可以有效防范各类网络威胁，确保信息化系统的稳定运行，为企业提供可靠的信息化服务和支持^[1]。

1.2 保护数据安全和隐私

随着互联网的普及和信息化技术的发展，大量的数据被传输、存储和处理。数据包含了个人隐私信息、商业机密以及敏感数据等，一旦泄露或被篡改会带来严重的后果。加强网络安全防护措施，建立数据加密、备份和恢复机制，可以有效保护数据安全，避免数据泄露和损坏，维护用户和企业的合法权益。

1.3 提升信息系统的抗风险能力

网络环境充满各种潜在的风险和威胁，如病毒攻击、网络钓鱼和数据劫持等，对信息系统造成了严重影响。通过建立健全的网络安全策略和应急响应机制，及时发现并应对网络安全事件，减轻风险影响，提升信息系统的抗风险能力。同时，定期进行安全演练和风险评估，积极应对不断演变的网络安全挑战，增强信息系统的应变和恢复能力，确保业务的持续性和稳定性^[2]。

2 信息化建设中网络安全分析

2.1 信息化建设概述

信息化建设是指利用信息技术和通信技术改进组织运作方式、实现业务流程优化和管理效率提升的过程。随着数字化时代的到来，信息化建设已成为各行各业发展的必然趋势。信息化建设不仅可以促进企业生产效率提升、降低成本，还可以加强企业与客户之间的沟通和互动，提升服务质量和竞争力。

在信息化建设中，网络扮演着关键角色，它是信息系统运行和数据传输的重要载体，连接了各种终端设备和应用系统，实现

【作者简介】张明（1987—），男，黑龙江大庆人，本科，中级工程师，研究方向：网络信息安全、信息化运行维护、视频监控等。

了信息资源的共享和交换。网络攻击、病毒感染、数据泄露等安全威胁给信息系统带来了巨大损失，严重影响了企业的正常运营和发展^[3]。因此，在信息化建设中，网络安全问题必须引起高度重视。应建立完善的网络安全体系，加密重要数据，制定合理的权限管理机制，定期进行漏洞扫描和安全评估，确保信息系统安全可靠运行。

2.2 网络安全现状分析

当今信息化建设环境下，网络安全问题日益突出，存在诸多问题，需要引起重视和关注。随着网络技术的不断发展，网络威胁也变得日益复杂多样化。恶意软件、网络病毒、勒索软件和网络钓鱼等各种网络攻击手段层出不穷，给企业和用户带来了巨大的安全风险。随着数据在网络中的快速传输和存储，数据泄密和隐私保护成为亟待解决的问题。尤其是在云计算、大数据时代，数据的安全存储和传输成为一项迫切需要解决的问题。除了技术层面的威胁外，社会工程和人为因素也是造成网络安全问题的重要原因。通过钓鱼邮件、社交工程等方式诱导用户泄露个人信息、登录密码等敏感信息，甚至利用员工的疏忽或无意识行为入侵系统。这种依托人为因素而发动的攻击手段更加隐蔽，更容易造成重大损失。

2.3 网络安全相关概念

2.3.1 防火墙 (Firewall)

防火墙是一种网络安全设备，用于监控和控制数据流量，根据预先设定的安全规则过滤和阻止不安全或未经授权的网络通信。防火墙可以解决黑客入侵、恶意软件传播和数据泄露等安全威

胁，是构建网络安全防护体系中的重要组成部分。

2.3.2 加密技术 (Encryption)

加密技术是网络安全领域中一种常用的手段，通过对数据加密处理，使未经授权的用户无法获取或理解数据内容。加密技术包括对称加密和非对称加密两种方式，用于保护数据在传输和存储过程中的安全性，防范数据被窃取或篡改。

2.3.3 漏洞 (Vulnerability)

漏洞指的是计算机系统或网络中存在的安全漏洞或缺陷，被黑客利用进行攻击。漏洞源自软件设计缺陷、配置错误和人为失误等原因，一旦发现并利用，就会给系统安全造成重大危害。定期漏洞扫描、修补漏洞以及加强安全意识培训是预防漏洞利用的主要手段。

2.3.4 木马 (Trojanhorse)

木马是一种常见的恶意软件，它表面上看起来像一个合法的程序，但实际上隐藏着恶意功能，可以盗取用户信息、破坏系统和远程控制等。防范木马侵袭应做好反病毒防护、定期系统清理检查等工作，避免木马对系统的危害。

3 信息化建设中网络安全与维护策略

3.1 网络安全防护策略

在信息化建设过程中，常见的网络安全风险包括黑客攻击、病毒感染、数据泄露和勒索软件等。黑客通过端口扫描、SQL注入和DDOS攻击等方式进入系统，制造混乱或窃取机密信息。病毒和勒索软件在系统中传播加密文件，导致系统瘫痪或数据丢失。数据泄露则因为缺乏加密保护或权限控制而发生泄露用户个人隐私或公司重要信息的问题。针对上述网络安全风险，黑客和恶意用户采用多种攻击手段，包括网络钓鱼、社会工程、恶意代码和漏洞利用等。网络钓鱼通过仿冒网站或虚假邮件诱导用户提供个人信息；社会工程利用心理学手段获取重要信息；恶意代码植入正常系统中，从内部破坏系统；漏洞利用则是利用系统中的漏洞入侵系统。

为了有效应对网络安全风险和攻击手段，信息化建设中应建立安全防护体系，包含安全防火墙、入侵检测系统和安全监控等设备，监控和防范网络入侵。对敏感数据进行加密处理，保护数据存储和传输过程中的安全。定期对系统和应用程序进行漏洞扫描和修复，及时堵塞系统漏洞。加强员工网络安全意识培训，防止点击恶意邮件或网页造成安全事件。制定综合的网络安全防护政策，采取多层次的安全防护措施，加强网络安全意识的培训，信息化建设能够更好地保障系统的安全性，提高网络安全防护的能力，确保信息系统的稳定运行和数据的安全保护^[4]。

3.2 网络安全监测与检测

网络安全监测是指通过实时监视和分析网络流量、系统日志和安全事件等数据，发现网络中存在的潜在威胁和异常行为，通常包括漏洞扫描、弱点评估和入侵检测等内容。通过网络安全监测系统，及时检测网络攻击、恶意软件感染和不明用户访问等异常情况，提前预警并采取相应的安全应对措施。网络安全检测是指利用安全检测工具和技术，对

系统和网络进行定期检测和扫描，发现安全漏洞、配置错误以及潜在风险，及时修复和加固系统，确保网络安全和稳定运行。

实现有效的网络安全监测与检测应建立完善的网络安全监测系统，包括入侵检测系统（IDS）、入侵防御系统（IPS）、安全信息与事件管理系统（SIEM）等，实现对网络流量和安全事件的实时监测分析。定期利用漏洞扫描工具、入侵检测系统对系统和应用程序进行全面检测和扫描，发现安全漏洞和弱点，及时修复和加强安全防护。建立健全的安全事件响应机制，明确安全事件处理的流程和责任，及时应对安全事件，最大程度减少安全风险对系统的影响。通过建立科学合理的网络安全监测与检测机制，企业和组织可以更好地发现和应对网络安全威胁，提高网络安全防护效果，保障信息系统的安全稳定运行。

3.3 网络安全应急响应

网络安全应急响应是在信息化建设中必不可少的一环，旨在及时有效处理网络安全事件和威胁，最大限度减少损失、恢复系统功能，保护数据安全。网络安全应急响应包括预案制定、事件检测、安全事件分析、应急响应和善后处置。首先，预案制定阶段应建立完善的网络安全应急预案，明确事件处理流程、责任分工和通信渠道，提前做好应对准备。其次，在事件检测过程中，通过实时监控日志、网络流量等信息，及时发现潜在的安全威胁和异常行为。最后，进行安全事件分析，对事件进行评估、分类和定级，确定应急响应优先级，制定具体的处置方案。

3.4 网络安全管理体系建设

优化网络安全与维护策略，建立完整的网络安全管理体系，提高网络安全的水平和管理效能。首先，明确和制定组织的网络安全政策和制度，明确网络安全目标、要求和责任，遵循网络安全的法律法规，为网络安全工作提供指导和规范。其次，对信息系统进行全面风险评估，识别潜在的安全威胁和漏洞，并根据评估结果制定相应的风险控制措施，确保网络安全风险可控并得到有效管理。再次，建立完善的权限管理和访问控制机制，根据不同岗位和用户角色进行权限划分，并限制对敏感数据和系统功能的访问，保护机密信息不被未经授权人员获取。另外，开展网络安全培训和教育，提高员工对网络安全的认知和意识，培养正确的安全行为习惯，减少内部因素对网络安全的威胁。最后，建立完善的安全事件响应机制，明确责任人员和处理流程，在网络安全事件发生时快速做出反应和处置，最大程度减少安全事件对系统造成的影响。

3.5 技术创新与网络安全

随着科技的不断进步和网络环境的快速发展，新型网络安全威胁和攻击手段不断涌现，因此技术创新成为应对挑战、提高网络安全水平的关键。利用新型安全技术如人工智能、区块链和物联网安全等，可以有效加大网络安全的防护力度。例如，人工智能技术可以实现智能异常检测和自动化安全响应，及时发现并应对安全威胁；区块链技术可以确保

数据的安全传输和存储，增强数据的完整性和可信度；物联网安全技术能够保护连接的设备和传感器免受入侵和攻击。加强数据加密技术的应用，保护数据在传输和存储过程中的安全性，有效防止数据泄露；网络隔离技术可以实现网络资源的分割和隔离，遏制横向扩散的网络攻击，发现并控制安全威胁。通过引入自动化安全监测系统和漏洞扫描工具，实现全天候的安全监控和漏洞检测，及时发现并修复系统和应用程序中的安全漏洞，降低被攻击的风险。

结语

随着信息技术的飞速发展和网络形势的日益复杂化，网络安全与维护已成为信息化建设中至关重要的环节。构建完善的网络安全管理体系、推动技术创新与网络安全、加强网络安全监测与检测、健全网络安全应急响应机制是提高网络安全水平、应对各类网络安全挑战的有效途径。^[5]

引用

- [1] 许俊良. 信息化时代下计算机网络安全问题分析[J]. 网络安全技术与应用, 2023(7):165-167.
- [2] 刘义. 医院信息化建设中的网络安全防护探究[J]. 网络安全和信息化, 2023(7):18-20.
- [3] 张堃. 计算机信息化技术应用及风险防控[J]. 信息记录材料, 2022, 23(1):155-157.
- [4] 陈华盛. 信息化时代计算机网络安全防护技术[J]. 数字技术与应用, 2021, 39(11):237-239.