 DOI: https://doi.org/10.12349/iser.v5i7.3101

Network Information Security Control Measures in Enterprise Informatization Construction

Yue Zhao

Air China Changchun Control Technology Co., Ltd., Changchun, Jilin, 130000, China

Abstract

In the construction of enterprise information, network information security control is very important, and some control measures need to be formulated. For example, strengthening network security infrastructure, such as deploying firewalls, intrusion detection systems, etc; Timely update system and software patches, fix security vulnerabilities; Implement strict access control and identity authentication mechanisms to prevent unauthorized access; Strengthen employee security awareness training, enhance employees' understanding and prevention ability of information security; Establish a security audit and monitoring mechanism to promptly identify and respond to potential security risks. Based on this, this paper analyzes the main factors affecting the network information security in the enterprise information construction, and puts forward its own suggestions for the network information security control measures in the enterprise information construction for reference.

Keywords

enterprise information construction; network information security; management control measures

企业信息化建设中的网络信息安全管控措施

赵越

中国航发长春控制科技有限公司，中国 · 吉林 长春 130000

摘　要

在企业信息化建设中，网络信息安全管控非常重要，需制定一些管控措施。例如，强化网络安全基础设施，如部署防火墙、入侵检测系统等；及时更新系统和软件补丁，修复安全漏洞；实施严格的访问控制和身份认证机制，防止未授权访问；加强员工安全意识培训，提高员工对信息安全的认识和防范能力；建立安全审计和监控机制，及时发现并应对潜在的安全风险。通过多种措施，可促进企业信息化建设的顺利进行。基于此，论文对企业信息化建设中影响网络信息安全的主要因素进行分析，并针对企业信息化建设中网络信息安全管控措施提出了自己的建议，以供参考。

关键词

企业信息化建设；网络信息安全；管控措施

1 引言

随着信息技术的迅猛发展和企业信息化建设的不断推进，网络信息安全问题逐渐严重。企业信息化建设中的网络信息安全不仅会影响企业的核心资产和商业秘密，还会涉及客户数据、供应链信息和运营流程等多个方面。一旦网络信息安全遭受威胁，会给企业带来巨大的经济损失和声誉风险。因此，采取有效的网络信息安全管控措施，可保护企业信息安全 [1]。论文主要研究企业信息化建设中影响网络信息安全的主要因素，企业信息化建设中网络信息安全管控措施，旨在帮助企业构建坚固的网络信息安全防线，保证企业信息化建设的稳健推进，为企业的长远发展保驾护航。

【作者简介】赵越（1988–），女，中国辽宁东港人，本科，工程师，从事网络安全研究。

2 企业信息化建设中影响网络信息安全的主要因素

2.1 技术漏洞与病毒攻击

在企业信息化建设中，技术漏洞与病毒攻击是影响网络信息安全的主要因素。技术漏洞主要源于软件或硬件设计上的缺陷，会被黑客利用，作为入侵企业网络的突破口。一旦漏洞被利用，黑客可以执行恶意代码、篡改数据、窃取敏感信息等，对企业造成严重的安全威胁。病毒攻击是通过传播恶意软件，如病毒、蠕虫、木马等，破坏企业网络系统的正常运行。病毒可以通过电子邮件、恶意网站、移动存储设备等途径进行传播，一旦感染企业网络，就会导致数据丢失、系统崩溃、网络瘫痪等严重后果。

2.2 人为操作失误或恶意行为

在企业信息化建设中，人为操作失误或恶意行为会影响网络信息安全。首先，人为操作失误主要源于员工对安全

规定的不了解、疏忽或技术能力不足。例如，员工可能不小心点击了含有恶意软件的链接，或者错误地将敏感信息发送给了未经授权的人员，从而给企业的网络安全带来威胁。其次，恶意行为指的是员工出于个人利益或其他目的，故意破坏企业的网络安全 [2]。例如，内部员工窃取公司机密、篡改数据或破坏系统，导致企业遭受重大损失。最后，还有一些外部攻击者可能利用社交工程手段，诱骗员工泄露敏感信息或执行恶意操作。

2.3 管理制度不完善

在企业信息化建设中，管理制度的不完善会影响网络信息安全。一个健全的管理制度能够为企业网络安全提供坚实的保障，但一旦制度存在缺陷或执行不力，就会给企业带来潜在的安全风险。首先，缺乏明确的网络安全政策，会导致员工对网络安全的认知模糊，很难形成有效的安全防范意识。其次，安全责任不明确，导致在出现安全问题时，无法快速定位问题源头，也很难追究责任。最后，缺乏有效的安全培训和教育机制，使员工缺乏必要的安全知识和技能，导致很难应对日益复杂的网络安全威胁。

2.4 外部威胁与攻击

在企业信息化建设中，外部威胁与攻击会对网络信息安全造成严重的影响。随着企业业务的扩展和互联网技术的发展，企业面临的外部威胁和攻击逐渐增多，外部的威胁和攻击往往来自黑客、恶意软件、病毒等。黑客会利用企业网络的漏洞，通过钓鱼、恶意软件等手段，窃取企业的敏感信息，如客户数据、财务数据、商业机密等，对企业造成重大损失。此外，黑客还会通过分布式拒绝服务（DDoS）攻击等手段，使企业网络陷入瘫痪，影响企业的正常运营 [3]。恶意软件和病毒也是企业网络安全的重大威胁。恶意程序会通过电子邮件、恶意网站、移动存储设备等途径传播，一旦感染企业网络，就会窃取企业信息、破坏系统文件、传播病毒等，给企业带来极大的安全隐患。企业的 IT 应用系统如图 1 所示。

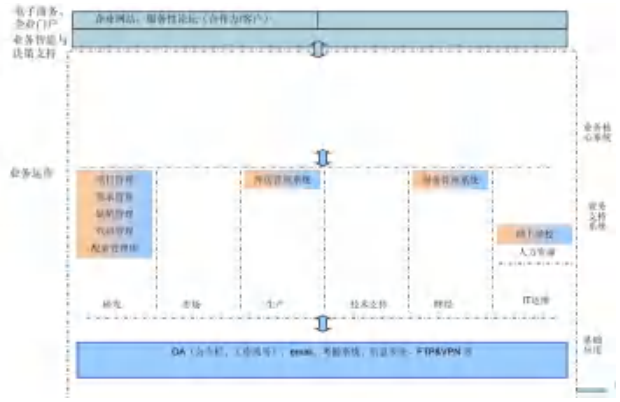

图 1 企业的 IT 应用系统

3 企业信息化建设中网络信息安全管控措施

3.1 加强网络安全基础设施建设

在企业信息化建设中，加强网络安全基础设施建设是保证网络信息安全的关键措施之一。随着信息技术的飞速发展，企业面对着逐渐增多的网络安全问题。首先，加强网络安全基础设施建设需要构建一个多层次的防御体系，主要包括部署防火墙、入侵监测系统等安全设备，实现对网络流量的实时监控和过滤，及时发现并阻止潜在的网络攻击。同时，还需要建立完善的网络安全管理制度，明确各级人员的安全职责和权限，保证各项安全措施得到有效执行。其次，随着云计算、大数据、人工智能等新一代信息技术的快速发展，企业可以充分利用这些技术来提升网络安全防护能力 [4]。例如，通过部署云安全解决方案，可以实现对企业云平台的全面保护；利用大数据分析技术，可以对网络流量进行深度挖掘和分析，发现潜在的安全威胁；通过人工智能技术，可以实现对网络攻击的智能识别和防御。最后，企业需建立完善的安全漏洞管理制度，及时发现并修复系统中的安全漏洞，防止黑客利用漏洞进行攻击。

图 2 网络安全基础设施建设图

3.2 强化系统安全更新和补丁管理

在企业信息化建设中，强化系统安全更新和补丁管理，有利于保证企业信息系统的稳固运行和数据安全。首先，企业需要建立一套完善的系统安全更新和补丁管理机制，机制包括定期扫描和检测系统漏洞、及时发布安全补丁，以及保证所有系统都能及时获得系统补丁。通过补丁管理机制，企

业可以及时发现并解决系统中的安全隐患，防止黑客利用漏洞进行攻击。其次，企业需对系统进行分类管理，根据系统的重要性和敏感性来设定不同的更新和补丁优先级。对关键业务和核心系统，应该设置更高的优先级，保证系统能够在最短时间内获得安全更新和补丁。最后，对于非关键系统，也要定期进行更新和补丁管理，消除潜在的安全风险。在实施系统安全更新和补丁管理时，要保证更新和补丁的来源可靠，避免安装恶意软件或病毒。在安装更新和补丁前，要对系统进行备份，以防万一出现更新失败或系统崩溃等问题[5]。在安装更新和补丁后，要对系统进行测试，保证系统的稳定性和性能没有受到影响。企业还需加强员工的安全意识培训。让员工了解系统安全更新和补丁管理的重要性，以及如何正确地进行相关操作。

3.3 严格访问控制和身份认证

在企业信息化建设中，网络信息安全是一项至关重要的任务。为了保障企业数据的机密性、完整性和可用性，严格的访问控制和身份认证成为网络信息安全管控的核心措施。一方面，严格的访问控制意味着对网络资源进行精细化的权限管理，要求企业根据员工的职责和需要，为员工分配不同的访问权限。例如，销售人员只能访问销售相关的数据，而财务人员只能访问财务数据。通过实施基于角色的访问控制（RBAC），企业可以更加灵活地管理员工的访问权限，保证每个员工只能访问其所需的信息，从而降低了信息泄露的风险。另一方面，身份认证是访问控制的基础。企业需采用多因素认证机制，如密码、生物识别、动态令牌等，保证访问者的身份真实可信。

3.4 加强员工的安全意识教育和培训

在企业信息化建设中，加强员工的安全意识教育和培训是保障网络信息安全的重要环节。随着信息技术的广泛应用，企业员工在日常工作中不可避免地会接触到企业的敏感数据和信息系统，因此，提升员工的安全意识，增强其对网络信息安全的认识和防范能力，对保护企业信息安全具有至关重要的作用。首先，企业应当明确安全意识教育和培训的重要性。安全意识教育和培训不仅能够帮助员工认识到信息安全对企业运营的重要性，还能够让员工了解到各种网络威胁的存在和防范方法。通过安全意识培训，让员工在日常工作中就能够更加警觉，避免因为疏忽大意而导致信息泄露或被攻击。其次，安全意识教育和培训应当具有针对性和实用性。企业应当针对员工的岗位职责和工作内容，制定相应的安全培训课程。例如，对于 IT 部门的员工，可以重点培训网络安全技术和攻防知识；对于非 IT 部门的员工，可以重点培训信息安全意识、密码保护、电子邮件安全等方面的知识。最后，培训应当注重实践操作，让员工在实践中掌握安全知识和技能。在安全意识教育和培训的过程中，企业还可以采用多种方式和手段。例如，可以组织员工参加网络安全知识竞赛、模拟攻防演练等活动，让员工在轻松愉快的氛围中学习和掌握安全知识。

3.5 安全审计、监控与外部合作

在企业信息化建设中，安全审计、监控与外部合作是保证企业信息安全的关键环节。首先，安全审计是企业网络信息安全管控的基础。安全审计涉及对企业信息系统的全面检查，包括系统配置、安全策略、访问控制、数据加密等方面。通过安全审计，企业可以及时发现系统存在的安全隐患和漏洞，从而采取相应的措施进行修复和改进。同时，安全审计还可以评估企业的信息安全管理体系是否完善，为企业的信息安全工作提供决策支持。其次，监控是保证企业网络信息安全的重要手段。企业需建立完善的网络安全监控系统，实时监测网络流量、安全事件和异常行为。通过监控，企业可以及时发现网络攻击、病毒传播等安全威胁，并采取相应的措施进行处置。再次，监控还可以帮助企业了解网络使用情况和性能状态，为企业的网络优化和升级提供依据。最后，外部合作是企业网络信息安全管控的必要补充。由于网络攻击和病毒传播等安全威胁往往来自外部，企业需要与专业的网络安全机构、安全厂商等建立合作关系，共同应对安全威胁。通过外部合作，企业可以获得专业的技术支持和安全保障，提高自身的信息安全防护能力。同时，外部合作还可以帮助企业了解最新的安全威胁和攻击手段，为企业的信息安全工作提供重要的情报支持。

4 结语

在企业信息化建设中，网络信息安全管控通过加强安全审计，实时监控潜在威胁，以及积极与外部安全机构合作，企业能有效降低信息安全风险。通过管控措施不仅保证了企业数据的安全性和完整性，也提升了企业的整体防御能力。同时，持续的员工安全意识培训使员工能够主动防范和应对网络安全风险，进而促进企业的信息化建设的顺利进行。

参考文献

[1] 董勇,张弛,叶水勇,等.电力企业终端信息安全风险分析与管控[J].电力与能源,2018,39(2):295-298.

[2] 杨艳萍.重载铁路装备企业安全信息化管理研究[J].装备制造技术,2023(8):240-242.

[3] 凌颖,刘振通,余通,等.基于网络信息设备资产的网络安全管理系统建设与应用[J].数码世界,2021(2):257-258.

[4] 赵国静,王东坡,旷文敏,等.安全生产风险防控体系及信息化平台的建设[J].化工管理,2022(13):121-124.

[5] 张喜刚.铁路企业安全管控3D建模对标消缺探索与实践[J].交通企业管理,2023,38(2):49-51.