ISSN: 2661-3719(Print); 2661-3727(Online)

“互联网+”背景下的网络信息安全及防护策略研究

吕晓霖　奚　悦
国网天水供电公司　甘肃天水　741000

摘　要：随着“互联网+”时代的到来，网络已经成为社会、经济和政治活动的核心。然而，伴随而来的是各种网络信息安全威胁，如数据泄露、黑客攻击和病毒传播等，对国家安全、企业经济和个人隐私构成了严重威胁。本研究深入探讨了“互联网+”时代背景下的网络信息安全问题，并提出了相应的防护策略。通过综合分析包括内外部威胁、安全技术、政策法规等多方面因素，旨在为中国当前的实际情况提供有针对性的信息安全解决方案。

关键词：互联网+；网络信息安全；防护策略；信息泄露；威胁分析；安全技术；政策法规

引言：

“互联网+”，这个概念已经深刻地改变了我们的社会和经济格局。随着数字技术的不断演进，互联网不再仅仅是信息传播的工具，它已经融入了几乎所有领域，从商业和政府到日常生活的各个层面。这一数字化浪潮不仅带来了便捷和机会，也引发了新的挑战，其中最重要的之一就是网络信息安全。在这个数字化时代，网络信息安全的保护变得尤为重要。互联网的广泛应用使得个人、组织和国家更加依赖于数字化数据的存储、传输和处理。然而，随之而来的是各种网络威胁，如数据泄露、黑客攻击和病毒传播，这些威胁对国家安全、企业经济和个人隐私构成了严重威胁。因此，本研究旨在深入探讨“互联网+”时代背景下的网络信息安全问题，并提出相关防护策略。有助于保护关键信息资产，维护国家安全，促进经济发展，同时也保障了个人隐私权。在下文中，我们将深入探讨网络信息安全的挑战、防护策略、案例分析以及未来趋势。

一、互联网+时代的网络信息安全挑战

1.新的威胁因素

在“互联网+”时代，网络信息安全面临了新的威胁因素。首先，大规模的数据数字化和云计算技术的普及使得大量敏感信息存储在云端，增加了数据泄露的风险。其次，物联网技术的兴起将各种设备连接到互联网，这些设备可能容易受到攻击，成为网络攻击的入口。最后，新兴技术如人工智能和区块链，尽管带来了创新，但也可能被恶意利用，导致新的安全挑战。

2.现状和趋势

信息安全问题的严重性可从各种网络安全事件中得以体现。不断有新闻报道指出企业遭受数据泄露，政府机构遭受黑客攻击，以及大规模病毒传播事件的发生。这些事件不仅导致了巨大的经济损失，还损害了企业和政府的声誉。

此外，网络犯罪的复杂性和普及性也在不断增加。黑客攻击手法不断升级，网络钓鱼、勒索软件、僵尸网络等威胁不断演进。同时，网络犯罪的国际性质也使打击这些犯罪行为变得更加复杂。

3.影响因素

网络信息安全问题的严重性不仅仅在经济层面体现，还对国家安全、企业经济和个人隐私产生深远影响。在国家层面，网络攻击可能导致关键基础设施的瘫痪，影响国家的政治稳定和社会安全。在企业层面，数据泄露和黑客攻击可能导致机密信息的泄露，竞争力的下降，甚至破产。在个人层面，隐私泄露可能导致个人身份被盗用，金融损失和个人尊严的丧失。[1]

二、网络信息安全威胁分析

在“互联网+”时代，网络信息安全威胁的多样性和复杂性不断增加。本节将详细分析各类网络信息安全威胁，包括内部和外部威胁，并通过提供真实案例和统计数据来支持威胁分析的论点。同时，我们将强调不同行业和领域的安全需求和风险的差异。

1.内部威胁

内部威胁源于组织内部的员工、合作伙伴或供应商，他们可能故意或无意中威胁网络信息安全。内部威胁的主要形式包括：

作者简介：
吕晓霖（1977.08）男，汉，籍贯：山东省莱州市，职称：副高，学历：本科，研究方向：信息网络。
奚悦（1996.09）女，汉，籍贯：甘肃省兰州市，学历：硕士，研究方向：信息技术。

数据泄露：员工、合作伙伴或供应商有可能泄露敏感信息，例如客户数据、财务信息等。

恶意行为：内部人员可能故意传播恶意软件、窃取机密信息或破坏网络系统，造成重大损失。

安全意识不足：员工对网络安全的重要性缺乏认识，可能会不小心点击恶意链接或共享敏感信息。

2.外部威胁

外部威胁涉及来自网络外部的恶意行为，攻击者通常是黑客、网络犯罪团伙或国家-sponsored攻击者。外部威胁的主要形式包括：

黑客攻击：黑客通过渗透网络系统来窃取信息、破坏系统或勒索受害者。

病毒和恶意软件：恶意软件可以传播病毒、勒索软件或间谍软件，威胁设备和数据的安全。

社交工程：攻击者利用欺骗手法获取信息，如钓鱼攻击、身份伪装等。

3.不同行业和领域的安全需求和风险

不同行业和领域面临着不同的网络信息安全需求和风险。例如，在金融领域，金融交易的安全性至关重要，而在医疗保健领域，患者数据的隐私和完整性是首要考虑因素。制造业可能面临工业间谍和供应链攻击的风险，而政府部门则需要保护国家安全和公共服务。

为了应对不同行业和领域的安全需求，必须根据其特定的风险制定相应的网络信息安全策略。

三、网络信息安全防护策略

网络信息安全的有效防护需要综合考虑多层次的策略，涵盖技术、管理和法律层面。本节将探讨这些策略，并介绍一些先进的安全技术，同时强调员工培训和安全意识的重要性，以及相关政策法规的合规性。

1.多层次的网络信息安全防护策略

技术层面：在技术层面，应采用多种安全措施来保护网络和数据。这包括使用防火墙来监控和过滤网络流量，入侵检测系统来识别异常行为，以及数据加密来保护敏感信息的传输和存储。

管理层面：在管理层面，需要建立完善的网络安全策略和程序。这包括访问控制、权限管理、安全审计和漏洞管理等。定期的风险评估和安全演练也是管理层面的重要组成部分。

法律层面：法律层面的防护策略包括遵守相关的网络安全法律和法规。中国的数据保护法和网络安全法对个人信息保护和网络安全提出了具体要求。组织需要确保自己的业务活动符合这些法律，以避免潜在的法律风险。

2.先进的安全技术

防火墙（Firewalls）：防火墙是网络安全的第一道防线，用于监控和过滤进出网络的流量，以防止未经授权的访问和攻击。

入侵检测系统（Intrusion Detection Systems，IDS）和入侵防御系统（Intrusion Prevention Systems，IPS）：这些系统用于检测和响应潜在的攻击和异常行为，帮助及时发现和阻止威胁。

数据加密：数据加密技术可确保数据在传输和存储过程中的机密性和完整性。加密算法和协议应与最新的安全标准保持一致。

3.员工培训和安全意识

无论多强大的技术措施，人员始终是网络信息安全的一环。员工培训和安全意识培养对于减少内部威胁和社交工程攻击至关重要。员工应接受定期的网络安全培训，了解如何识别威胁、遵守安全政策和报告可疑活动。

4.政策法规合规性

中国的数据保护法和网络安全法明确规定了个人信息保护和网络安全的要求。组织需要了解并遵守这些法律，确保其数据处理和网络操作合规。同时，建立内部合规团队和流程，以应对可能的法律审查和合规性审计。[2][3]

四、互联网+时代的网络信息安全案例研究

在“互联网+”时代，网络信息安全案例研究是了解成功和失败的关键因素以及获得实际经验和教训的有效途径。本章将深入研究一些代表性的网络信息安全案例，分析它们背后的因素，并提供案例研究的实际教训和应用经验。

1.成功案例：Apple的数据隐私保护

案例背景：Apple公司一直致力于保护用户的数据隐私，尤其是在移动设备上。其最显著的举措之一是引入了隐私标签（Privacy Labels）的概念，要求在App Store中向用户提供应用的数据收集和隐私政策信息。

成功因素：

用户优先：Apple将用户的隐私放在首位，始终坚守“数据属于用户”的原则。这为公司赢得了用户的信任和忠诚。

透明度和可控性：引入隐私标签和数据控制工具，赋予用户更多的数据控制权和透明度，让用户能够更好地管理其个人信息。

法规合规：Apple积极响应全球数据隐私法规，确保其产品和服务在全球范围内都符合法律要求。

用户信任至关重要：公司应该坚守用户隐私保护的原则，积极采取措施来赢得用户的信任，这将有助于维护声誉和市场竞争力。

透明度和控制权：提供用户更多的透明度和控制权，是维护用户信任的关键。为用户提供简明扼要的隐私政策和数据管理工具。

2.失败案例：Equifax的数据泄露

案例背景：Equifax是一家信用评级机构，2017年发生了严重的数据泄露事件，导致约147万用户的敏感信息泄露，包括社保号码、信用卡信息等。

失败因素：

不足的安全措施：Equifax在数据安全方面采取了不足的措施，未能及时发现并应对安全漏洞。

不及时的通知：公司未能及时向受影响的用户通知数据泄露事件，导致用户无法采取及时的措施保护自己的信息。

及时的通知和合规：在发生数据泄露事件时，公司应该立即采取措施通知受影响的用户，并确保合规性，以避免法律后果。

五、未来趋势和建议

网络信息安全领域在不断演进，未来将受到新技术和威胁的影响。在本节中，我们将展望未来网络信息安全的发展趋势，并提出一些关于网络信息安全的未来建议，包括研究方向、政策制定和技术投资等方面的建议。

1.未来发展趋势

人工智能（AI）和机器学习（ML）：AI和ML将在网络信息安全中扮演更重要的角色，用于检测和应对威胁。这些技术可以自动分析大量数据，识别异常行为，并快速响应威胁。

物联网（IoT）安全：随着物联网设备的爆发性增长，物联网安全将成为一个重要关注点。保护设备、传感器和连接性将是未来的挑战。

2.未来建议

加强研究和创新：政府和企业应继续支持网络信息安全领域的研究和创新。投资于新技术和安全解决方案的研发，以不断适应威胁的演化。

跨界合作：国际合作在网络信息安全方面至关重要。建立国际标准、信息共享和联合行动将有助于更好地应对跨国网络犯罪。

政策制定和法规：政府应制定更加严格的网络信息安全法规，以确保组织遵守最佳实践。同时，政策应促进个人信息保护和数据隐私。

安全教育和培训：组织应继续投资于员工网络安全教育和培训，提高他们的安全意识和技能。

紧急响应计划：开发和测试网络信息安全的紧急响应计划是至关重要的。在威胁发生时，迅速、有效地应对是减少损失的关键。[4]

六、结论

本研究深入探讨了“互联网+”时代下网络信息安全的问题和解决策略，我们总结如下：

通过分析内外部威胁、安全技术、政策法规等因素，我们认识到网络信息安全在当前社会、经济和政治活动中的关键性。新挑战如数据泄露、黑客攻击和病毒传播等威胁国家安全、企业经济和个人隐私。为了有效应对这些挑战，我们提出了多层次的网络信息安全防护策略，包括技术、管理和法律层面。综上所述，网络信息安全是一个不断演进的领域，需要我们不断改进策略、创新技术，以适应新的挑战和威胁。在保护关键信息资产和个人隐私的同时，我们也需要共同努力，为网络信息安全建设提供坚实的基础。

参考文献：

[1]任伟.计算机网络信息安全及防护策略研究[J].数码世界，2019（07）：244.

[2]唐丽丽.新时期互联网云计算的防护体系探索[J].网络安全技术与应用，2017（04）：120+124.

[3]盘点那些置我们于危险之中的信息泄露事件[J].大数据时代，2018（08）：64-73.

[4]顾正庶.互联网中信息安全技术的重要性及其应用[J].山东工业技术，2019（04）：138.