针对信创系统网络安全问题及策略分析

崔洁
北京华科软科技有限公司

摘　要：在当今数字化时代，信息技术的快速发展已经使信创系统（信息技术创新系统）成为国家经济和国防战略的关键组成部分。信创系统不仅催生了大量科技创新，还在各个领域推动了经济的增长和社会的进步。然而，随着信创系统的广泛应用和依赖，网络安全问题也日益突出。本文详细分析了外部和内部网络安全威胁，提出了一系列网络安全策略及管理措施，旨在为信创系统的网络安全提供深入洞察和有实际应用价值的建议，以确保其在不断发展的信息时代中保持安全稳定。

关键词：信创系统；安全威胁；安全策略；安全管理
【DOI】10.12252/j.issn.2096-6288.2022.12.109

引言

网络安全问题一直以来都备受关注，但在信创系统背景下，这些问题变得更加严重和复杂。网络黑客、恶意软件、社会工程攻击等威胁不断演变，威胁着信创系统的安全和稳定性。此外，内部威胁如员工疏忽和错误、内部恶意行为也不容忽视，它们同样对信创系统的安全构成了威胁。本文旨在深入研究信创系统中的网络安全问题，并提供相应的策略分析，希望能够为企业、政府和个人提供有效的网络安全解决方案，确保其在数字化时代的可持续发展。

一、信创系统网络安全威胁分析

（一）外部威胁

（1）恶意软件

恶意软件（Malware）是一类恶意设计的软件，其目的是对系统、数据和用户造成损害。恶意软件可以采取各种形式，包括病毒、蠕虫、特洛伊木马、间谍软件、广告软件等。这些恶意软件可以通过多种途径传播，例如恶意附件、感染的链接、恶意广告或不安全的下载。恶意软件的危害多种多样，可以窃取敏感数据，如个人身份信息、信用卡信息、登录凭证等，然后将其传送给攻击者，可能导致严重的隐私问题和经济损失。恶意软件还会破坏计算机系统的正常运行，导致系统崩溃、文件损坏或无法访问，对业务和个人产生重大影响。恶意软件可以用于发动网络攻击，如分布式拒绝服务（DDoS）攻击，使网络资源不可用，影响服务可用性。恶意软件中的勒索软件（Ransomware）可以加密用户文件，然后勒索用户支付赎金以获取解密密钥，这种勒索行为已经导致了许多组织和个人遭受巨大损失。

（2）网络攻击

网络攻击是利用系统的漏洞或弱点，以获取未经授权的访问、窃取敏感信息或损害系统的可用性。网络攻击的形式多种多样，包括但不限于恶意软件传播、数据泄漏、拒绝服务攻击（DDoS）、勒索软件攻击等。网络攻击者通常具有广泛的技术知识，可以利用各种工具和技术来入侵系统，可能会针对特定的目标进行攻击，也可能进行大规模的随机扫描以找到易受攻击的系统。攻击者的动机各不相同，包括经济利益、政治动机、破坏行为等。在信创系统中，网络攻击可能导致严重的后果，如数据丢失、用户隐私泄漏、服务中断、声誉损失等。因此，了解不同类型的网络攻击、及时识别和应对攻击至关重要。网络安全策略和措施应该包括防御措施，例如防火墙、入侵检测系统（IDS）、入侵防御系统（IPS），以及监控和响应机制，以便及时发现和应对潜在的网络攻击。

（3）社会工程攻击

社会工程攻击是一种攻击者通过欺骗、操纵、或诱导人们来揭示敏感信息或执行恶意操作的手段，这种攻击通常不涉及技术漏洞，而是利用人的天性，如好奇心、善意或者轻信，来获取访问权限或敏感信息。社会工程攻击的形式多种多样，包括钓鱼邮件、电话欺诈、伪装成信任的实体、欺骗性社交工程等等。攻击者可能冒充银行员工，要求用户提供银行账户信息，或者发送伪装成合法网站的电子邮件，引诱用户点击恶意链接，还可以通过社交媒体信息来收集关于个人的信息，以更有针对性地进行攻击。社会工程攻击的危险性在于，不仅可以直接导致信息泄漏和数据损失，还可以为其他更严重的网络入侵行为铺平道路。因此，教育和培训员工，以提高他们对社会工程攻击的警觉性，是网络安全战略中的一个重要组成部分。

（二）内部威胁

（1）员工疏忽和错误

员工作为组织内部的一部分，其行为和决策可能对网络安全产生直接影响，员工疏忽和错误通常包括以下情况。员工训练不足：员工可能没有接受充分的网络安全培训，导致他们对网络安全最佳实践和政策不够了解。在缺乏培训的情况下，员工可能不知道如何正确处理敏感信息、识别恶意电子邮件或报告潜在的安全威胁。忽视安全政策：尽管组织可能已经制定了明确的网络安全政策和程序，但员工有时可能忽视这些政策，因为他们觉得这些政策会妨碍他们的工作效率。例如，他们可能会绕过多层次的身份验证，共享敏感信息，或者使用不安全的密码。点击恶意链接：员工可能会因为不小心或缺乏警觉性而点击恶意链接或打开恶意附件，从而导致恶意软件的传播或网络攻击的成功。弱密码和身份验证：一些员工可能会使用弱密码，或者共享他们的凭据，以便其他人可以访问他们的账户，这种行为可能会被恶意攻击者滥用，进而导致数据泄漏或未经授权的访问。

（2）内部恶意行为

内部恶意行为是指组织内部员工或其他授权人员，故意或非故意地从事危害组织信息安全的活动。这种行为可能由多种因素驱动，包括不满、个人动机、经济诱因、无知、社会工程攻击、疏忽或错误等。内部恶意行为可能表现为数据泄漏、故意破坏、未经授权的系统访问、滥用权限、盗窃机密信息、篡改数据、擅自共享敏感信息等。这些行为不仅对组织的声誉和财务状况构成威胁，还可能违反法律法规，导致法律后果。为应对内部恶意行为，组织需要采取一系列措施，包括实施访问控制和权限管理、监控员工活动、建立报告机制、提供安全意识培训、制定行为准则和政策、进行内部审计等。

二、信创系统网络安全策略

（一）防御策略

（1）网络边界防御

网络边界防御旨在保护信创系统的核心网络和数据免受外部威胁和攻击的侵害，网络边界防御采用一系列技术和措施来筛选和阻止恶意流量进入信创系统的网络环境，包括防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等安全设备和应用程序，这些设备和应用程序能够监视网络流量、分析数据包，并根据事先设定的安全策略来阻止潜在威胁。防火墙作为第一道防线，根据规则集来允许或拒绝特定流量。入侵检测系统能够识别异常行为和攻击模式，而入侵防御系统则能主动阻止恶意流量，增强网络的安全性。此外，网络边界防御还包括对入口点的严格访问控制，以确保只有经过授权的用户和设备能够访问信创系统的网络资源。这可以通过身份验证和授权机制、虚拟专用网络（VPN）、双因素认证等方法来实现。

（2）内部安全措施

内部权限管理是一项重要的内部安全措施，旨在限制员工和用户访问系统和数据的权限。通过实施适当的权限管理，可以确保只有经过授权的个人可以访问敏感数据和系统功能，涉及角色基础的访问控制（RBAC）和最小权限原则的应用，以确保员工只能访问与其工作职责相关的信息。安全审计和监控是另一个内部安全措施的关键组成部分，包括定期审计系统和应用程序的活动，以检测潜在的异常行为或安全漏洞。监控系统可以及时发现并响应任何异常活动，从而减少潜在的风险。此外，日志记录和事件管理系统有助于跟踪系统的活动，以便在需要时进行调查和回溯。员工培训和教育也是内部安全措施中的一个关键方面。通过为员工提供关于网络安全最佳实践、识别威胁的培训以及如何安全使用公司资源的教育，可以提高员工对网络安全的意识，并降低社会工程攻击等风险。

（二）检测与响应策略

（1）威胁检测

威胁检测是一个综合性的过程，旨在识别潜在的网络威胁和攻击，以便及时采取措施进行应对。在信创系统中，威胁检测需要考虑外部威胁，包括来自恶意软件、网络攻击和社会工程攻击的威胁。恶意软件可能以各种形式存在，包括病毒、木马、恶意脚本等，因此威胁检测系统需要能够识别并阻止这些恶意代码的传播和执行。此外，网络攻击也是一个常见的威胁，攻击者可能试图入侵系统、窃取敏感信息或破坏系统正常运行。社会工程攻击则是利用人员的社会工程学弱点，通过欺骗或诱导来获取访问权限或信息。威胁检测还需要关注内部威胁，包括员工的疏忽和错误以及内部恶意行为。员工可能无意中泄漏敏感信息或采取不安全的行为，因此威胁检测系统需要监测并纠正这些问题。另外，内部恶意行为可能来自公司内部的员工或合作伙伴，他们可能试图窃取数据、损害公司声誉或从内部发起攻击。威胁检测需要监测不寻常的活动或异常行为模式，以及尽早发现并应对这些威胁。

（2）事件响应

事件响应是指在网络发生安全事件或威胁时，组织

采取的一系列步骤和措施，以快速识别、分析、应对和恢复从事件中受到的损害，主要包括以下几个方面。事件检测和识别：及时检测并识别网络安全事件，可以通过使用安全信息和事件管理系统（SIEM）、入侵检测系统（IDS）、入侵防御系统（IPS）以及其他监测工具来实现，这些工具可以监视网络流量、系统日志和异常行为，以便迅速发现潜在的问题。事件分类和分级：一旦发现安全事件，应该对其进行分类和分级，以确定事件的重要性和紧急性，有助于确保适当的资源分配和响应优先级。事件分析：对事件进行深入分析，以确定事件的性质、攻击者的方法和目标。事件响应计划：在事件发生之前，组织应该制定事件响应计划，明确定义每个阶段的任务和责任，包括确定谁负责采取行动、如何通知相关方和如何保护系统和数据。威胁缓解和恢复：一旦了解了事件的性质，应采取适当的措施来缓解威胁并恢复受到影响的系统和数据，包括隔离受感染的系统、修复漏洞、还原备份数据等。

（三）安全意识培训策略

安全意识培训旨在提高组织内部员工对网络安全风险和最佳实践的认知，并教育他们如何正确应对潜在的威胁，核心目标是构建安全意识的文化，使所有员工都能积极参与和贡献到网络安全的维护中。首先，需要开发精心设计的培训课程，以涵盖各种网络安全主题，包括密码管理、社会工程攻击识别、恶意软件防范等。这些课程应当适应不同员工群体的需求，从高管到基层员工都应考虑。其次，安全意识培训策略需要使用多种教育工具和方法，以确保培训的多样性和吸引力，包括在线培训模块、模拟演练、定期会议、内部通讯和邮件提醒等。此外，通过定期的测试和评估，可以测量员工的安全意识水平，并识别需要进一步加强的领域。最后，领导层的积极支持和示范对于安全意识培训的成功至关重要，高级管理人员应该充当榜样，积极参与培训，并强调网络安全对整个组织的重要性。

三、信创系统网络安全管理

（一）安全政策和流程

安全政策和流程为组织提供了指导和框架，以确保网络安全措施得以实施和维护。安全政策应明确定义组织对网络安全的承诺和期望，包括明确陈述组织对网络安全的重要性，以及高层管理层对安全的支持和承诺。安全政策还应规定了组织的目标和目标，明确了要保护的关键资产和信息。安全政策还应包括对风险管理的方法，包括评估和识别潜在的网络安全威胁和漏洞，以及采取措施来减轻风险和应对安全事件的计划。此外，安全政策还应明确安全责任和权限，确定谁有权访问、管理和监控网络和系统，以及如何分配安全任务和职责。

（二）安全技术和工具

安全技术和工具旨在提高系统的安全性，检测潜在的威胁并应对攻击。在信创系统的网络安全管理中，安全技术和工具的有效使用是确保数据和系统保持安全的关键要素。安全技术方面，包括入侵检测系统（IDS）和入侵防御系统（IPS），这些系统能够监测网络流量和系统活动，识别异常行为并采取必要的措施来应对潜在的攻击。另外，防火墙技术也是保护网络的关键，可以配置规则来控制流经网络的数据包。加密技术用于保护数据的机密性，确保敏感信息不会在传输过程中被窃取或篡改。工具方面，网络安全团队使用各种安全工具来管理和监控系统。漏洞扫描工具可以帮助识别系统中的潜在漏洞，从而及时修复它们。日志管理和分析工具用于跟踪系统活动，帮助检测不寻常的行为和安全事件。身份验证和访问控制工具确保只有授权的用户能够访问敏感数据和系统资源。

四、结语

综上所述，信创系统在今天的数字化环境中面临着不断增加的网络安全威胁。外部威胁如恶意软件和网络攻击，以及内部威胁如员工疏忽和内部恶意行为都对系统的安全构成潜在风险。为了应对这些威胁，信创系统需要采用多层次的网络安全策略，包括防御、检测与响应、以及安全意识培训。此外，有效的网络安全管理和合规性措施也是确保系统安全的关键。随着新兴威胁和技术趋势的不断演变，信创系统需要保持警惕，不断升级和改进其网络安全策略，以确保系统的持续安全和稳定。

参考文献

[1]李果.终端安全管理系统在企业中的应用[J].江西电力职业技术学院学报，2020，01.

[2]丁宇亮，张博.档案管理系统的智能化和自动化改进设计[J].信息与电脑（理论版），2022，19.

[3]胡旭斌.基于信息技术的安全管理系统建设[J].计算机与网络，2021，14.

[4]赵俊，瞿伟峰.探讨信创系统网络安全问题及策略[J].网络安全技术与应用，2022（04）：11-12.

[5]周栋.信创混合云管理平台的设计与实现[J].信息系统工程，2022（03）：52-55.