公路运输信息化中的网络安全问题及对策研究

蒋燕敏
嘉兴市公路与运输管理中心　浙江　嘉兴　314031

摘　要：随着信息技术的飞速发展，公路运输行业逐步迈向信息化，极大地提高了运输效率和管理水平。然而，信息化进程中也伴随着严峻的网络安全问题，如数据泄露、系统漏洞、IP被盗及病毒入侵等，这些问题直接威胁到公路运输行业的正常运转和信息安全。本文旨在深入探讨公路运输信息化中的网络安全问题，并提出相应的对策措施，以期为该行业的健康发展提供理论参考和实践指导。

关键词：公路运输；信息化；网络安全；问题；对策

引言

公路运输作为国民经济的重要支撑，其信息化进程对于提升运输效率、优化资源配置具有重要意义。然而，随着信息化程度的加深，网络安全问题日益凸显，成为制约公路运输信息化发展的重要因素。因此，研究公路运输信息化中的网络安全问题及对策，对于保障行业信息安全、推动行业可持续发展具有重要意义。

1 公路运输信息化中的网络安全问题

1.1 数据安全问题

1.1.1 数据泄露与丢失

当前，虽然许多公路运输管理事业单位已经引入了信息化管理系统，但在系统安全性方面仍存在诸多挑战。这些系统往往缺乏先进、完善的安全防护措施，导致数据泄露和丢失的风险依然较高。具体来说，由于缺乏有效的数据加密和访问控制机制，敏感数据如公路信息、车辆信息、运输记录、个人信息等可能在不经意间被泄露给未经授权的第三方。同时，数据备份和恢复机制的不完善也使得在数据丢失后难以迅速恢复，给单位的正常运转带来极大的不确定性和风险。

1.1.2 数据篡改

在物联网技术广泛应用于公路运输的背景下，传感器节点成为数据传输的重要组成部分。然而，这些传感器节点由于暴露在外部环境中，容易受到恶意攻击。攻击者可能通过篡改传感器节点传输的数据，来影响公路检测系统的准确性和可靠性[1]。例如，可能恶意修改传感器收集的关于公路和桥梁状态的数据，导致相关部门无法准确掌握公路和桥梁的真实状况。这样一来，公路养护和桥梁维护工作就可能因为缺乏准确的数据支持而变得不到位，进而影响道路的安全性和使用寿命。这种数据篡改不仅会影响公路运输的正常秩序，还可能对道路安全构成严重威胁。因此，必须加强对传感器节点的安全保护，确保数据的真实性和完整性。

1.2 系统漏洞问题

1.2.1 系统漏洞严重

公路与运输管理单位的信息系统往往承载着大量的敏感数据和关键业务，然而，这些系统却常常存在严重的安全漏洞。这些漏洞可能源于软件开发过程中的疏忽、配置不当、或是使用了存在已知漏洞的第三方组件。黑客利用这些漏洞，可以轻易地绕过安全机制，窃取重要信息，甚至对系统进行破坏，导致单位业务中断，造成不可估量的损失。更为严重的是，一些黑客可能利用这些漏洞进行勒索或恶意攻击，进一步加剧安全风险。

1.2.2 系统更新滞后

面对系统漏洞，及时修复和升级是保障系统安全的有效手段。然而，部分公路与运输管理单位对系统漏洞的认识不够深刻，缺乏足够的安全意识和紧迫感。他们可能忽视系统更新的重要性，或是担心更新会影响业务连续性而迟迟不采取行动。这种滞后更新的做法，使得系统长时间暴露在已知漏洞的风险之下，为黑客提供了可乘之机。此外，一些单位即使进行了更新，也可能由于操作不当或配置错误，导致更新未能有效生效，从而无法真正提升系统的安全性。

1.3 人员安全意识薄弱

1.3.1 安全意识不强

在单位内部，部分员工对于网络安全的认识尚显不足，缺乏基本的安全意识。他们在使用电脑、手机等设备时，往往忽视安全警告，随意下载未知来源的软件，甚至点击垃圾邮件中的链接。这种行为极易导致恶意软件的入侵，不仅可能损害个人设备，更可能将单位网络置于风险之中。一旦恶意软件在单位网络内传播，可能会窃取敏感信息，破坏系统功能，甚至导致整个网络的

瘫痪。

1.3.2 培训不足

除了安全意识不强外，单位在网络安全培训方面的投入也不足。许多员工对于网络安全的基本知识、操作技能以及应急处理方法知之甚少。在面对网络攻击时，他们往往束手无策，无法有效地应对和处置。这种培训不足的情况不仅降低了员工的安全防范能力，也增加了单位网络的安全风险。

1.4 资源共享安全隐患

由于各单位信息化建设的步伐不一，采用的技术平台、数据格式及标准存在显著差异，这直接导致了数据共享上的技术壁垒。例如，一些单位可能采用较为先进的云计算平台，而另一些则仍依赖于传统的本地服务器，这种差异使得数据在传输和整合时面临兼容性问题。此外，数据标准的多样化也增加了数据解析和处理的复杂度，降低了数据共享的效率。更为复杂的是，在数据共享过程中，如何确保数据的安全性和合法性成为一大挑战[2]。数据在传输途中可能遭遇拦截、篡改或非法访问，特别是在涉及车辆位置、乘客隐私等敏感数据时，一旦泄露将对企业运营和个人造成严重影响。同时，不同单位间对于数据使用的法律边界和合规要求理解不一，缺乏统一的数据共享协议和法律法规指导，增加了数据共享的法律风险。

2 公路运输信息化中网络安全问题的对策措施

2.1 加强数据安全管理

2.1.1 完善数据保护措施

为了切实保障数据的安全与完整，必须采取一系列严密的数据保护措施。首要任务是对所有敏感数据实施加密处理，这一步骤至关重要。应选用先进的加密算法，如AES或RSA，确保数据在传输及存储环节中均得到强有力的保护，有效抵御未经授权的访问。同时，密钥管理同样不容忽视，应建立定期的密钥更新机制，进一步提升数据的安全性，防止因密钥泄露而引发的风险。此外，构建完善的数据备份与恢复体系也是关键一环。需制定详尽的备份策略，确保备份数据能够全面覆盖所有关键信息，并且备份过程应自动化执行，以减少人为操作失误。备份数据应存储在安全可靠的地点，如异地灾备中心，以防范本地灾难性事件的影响。同时，定期对备份数据进行恢复测试，验证其完整性和可用性，确保在真实灾难发生时，数据能够迅速且准确地恢复。最后，加强敏感数据的访问控制同样重要。通过实施严格的权限管理、身份认证以及审计机制，确保仅有授权人员能够访问及操作数据，从而有效防止数据泄露和滥用。

2.1.2 推进信息化管理

为了从根本上解决数据安全问题，必须加快信息化系统建设步伐。首先，应明确系统需求，结合单位实际业务情况定制开发信息系统。在系统设计过程中，应充分考虑数据安全的需求，将数据加密、访问控制等安全机制融入系统架构中。同时，系统应具备完善的功能，能够满足单位在数据管理、业务处理等方面的需求，提高工作效率和准确性。其次，在信息系统建设过程中，应采用先进的技术平台和标准化的数据格式，以确保系统的兼容性和可扩展性。这有助于降低数据共享的难度，提高数据整合和处理的效率。最后，应加强对信息系统的运维管理，定期进行系统更新和漏洞修复，确保系统的稳定性和安全性。同时，还应建立完善的应急响应机制，以应对可能发生的网络安全事件，确保单位的正常运转。

2.2 强化系统漏洞管理

2.2.1 定期排查漏洞

建立系统漏洞定期排查机制是强化系统漏洞管理的首要步骤。这一机制应涵盖所有关键信息系统和基础设施，确保每一个角落都得到充分的关注。排查过程中，应利用专业的漏洞扫描工具和技术，对系统进行全面而深入的检测。这些工具能够识别出系统中存在的已知漏洞和潜在弱点，为后续的修复工作提供准确的信息。在排查出漏洞后，必须立即进行修复。修复工作应根据漏洞的严重程度和紧急程度进行优先排序，确保最严重的漏洞得到及时处理。修复过程中，应遵循最佳实践和安全标准，确保修复措施的有效性和可靠性[3]。同时，还应建立漏洞修复跟踪机制，对修复进度和结果进行实时监控和记录，确保所有漏洞都得到妥善处理。

2.2.2 加强系统更新升级

除了定期排查漏洞外，加强系统更新升级也是强化系统漏洞管理的重要措施。随着技术的不断发展和黑客攻击手段的不断演变，系统必须不断更新升级以应对新的安全威胁。因此，应密切关注行业动态和技术发展，及时获取最新的安全信息和更新补丁。在更新升级过程中，应采取谨慎和稳健的策略。首先，应对更新补丁进行充分的测试和验证，确保其稳定性和兼容性。这有助于避免更新过程中可能出现的系统崩溃或功能异常等问题。其次，应制定详细的更新计划和方案，明确更新的时间表、步骤和回滚措施。这有助于确保更新过程的顺利进行，并在出现问题时能够及时恢复系统。此外，还应加强对第三方组件和依赖库的管理。这些组件和库是系统的重要组成部分，但也可能成为黑客攻击的突破

口。因此，应定期检查和更新这些组件和库，确保其安全性和稳定性。同时，还应建立与第三方供应商的合作机制，及时获取安全信息和更新支持。

2.3 提升人员安全意识

2.3.1 加强安全培训

为了增强员工的安全意识，必须定期组织网络安全培训。这些培训应涵盖网络安全法律法规、安全操作规范以及应急演练等多个方面。通过法律法规的培训，员工可以了解到网络安全的重要性和违反安全规定的法律后果，从而增强遵守安全规定的自觉性。安全操作规范的培训则可以让员工掌握正确的操作方法和流程，避免因操作不当而引发的安全风险。应急演练是提升员工应急处理能力的重要手段。通过模拟真实的网络安全事件，让员工在实战中学习和掌握应急处理的方法和技巧。这不仅可以提高员工的应变能力，还可以检验和完善应急预案的有效性和可行性。为了确保培训的效果，应定期对培训内容进行更新和优化，以适应不断变化的网络安全环境。同时，还可以采用多种培训方式，如在线学习、专家讲座、实操演练等，以满足不同员工的学习需求和偏好。

2.3.2 建立安全责任制

为了确保网络安全责任落到实处，必须建立明确的安全责任制。这包括明确各部门、各岗位的网络安全职责和权限，以及将网络安全纳入绩效考核体系。通过明确职责和权限，可以让每个员工都清楚自己在网络安全方面的责任和义务，从而增强安全意识和责任感。将网络安全纳入绩效考核体系，则可以将安全责任与员工的切身利益相挂钩，进一步激发员工履行安全责任的积极性和主动性。在实施安全责任制的过程中，还应加强监督和检查。通过定期对各部门、各岗位的安全工作进行检查和评估，可以及时发现和纠正存在的问题和不足，确保安全责任得到有效落实。同时，还可以建立奖励和惩罚机制，对在网络安全工作中表现突出的员工进行表彰和奖励，对违反安全规定的员工进行批评和处罚，从而形成良好的安全文化氛围。

2.4 优化资源共享机制

2.4.1 建立统一数据标准

数据标准的统一是实现资源共享的基础。为了加强与相关单位的数据共享协同，必须建立统一的数据标准和格式。这包括明确数据的命名规则、数据结构、数据类型等方面的要求，以确保数据在传输和整合时具有一致性和兼容性。在建立统一数据标准的过程中，应充分考虑各单位的实际情况和需求，通过协商和沟通达成一致。同时，还可以借鉴行业内的最佳实践和标准，以确保数据标准的先进性和实用性。统一数据标准的实施不仅可以提高数据共享的便利性和效率，还可以降低数据解析和处理的复杂度，减少因数据格式不一致而导致的错误和冲突。

2.4.2 加强数据共享监管

数据共享过程中的安全监管是确保数据不被滥用和破坏的关键。为了加强数据共享的监管，必须制定数据共享安全规范和政策。这些规范和政策应明确数据共享的原则、范围、方式以及安全要求等方面的内容，为数据共享提供指导和约束。在数据共享过程中，应加强对数据访问、传输、存储和使用等环节的监控和管理。通过采用身份认证、访问控制、数据加密等安全措施，确保数据在共享过程中的安全性和保密性[4]。同时，还应建立数据共享审计机制，对数据共享的行为进行记录和审计，以便在出现问题时能够及时追溯和定位。除了技术层面的监管外，还应加强法律和政策层面的监管。通过制定和完善相关法律法规和政策，明确数据共享的法律责任和义务，为数据共享提供法律保障。同时，还应加强对数据共享活动的监督和检查，确保各单位遵守数据共享的安全规范和政策，维护数据的合法性和权益。

结语

公路运输信息化中的网络安全问题是一个复杂而重要的任务。通过加强数据安全管理、强化系统漏洞管理、提升人员安全意识以及优化资源共享机制等措施，可以有效解决这些问题，提高公路运输管理事业单位的工作效率和服务质量。未来，随着技术的不断进步和管理的不断完善，公路运输行业的网络安全问题将得到更好的解决，为行业的健康发展提供有力保障。

参考文献

[1]韩国俊.公路运输经济发展中的信息化管理挑战与对策研究[J].运输经理世界,2024,(01):68-70.

[2]蒙红妙.交通运输中网络信息安全策略运用分析[J].通讯世界,2024,31(03):51-53.

[3]马季.交通运输中的网络安全状况与对策分析[J].电子技术,2022,51(09):212-213.

[4]马季.网络信息安全策略在交通运输中的应用[J].集成电路应用,2022,39(08):142-143.