

网络安全态势感知下的交通运输风险预防措施

——评《交通运输行业网络安全态势感知技术研究》

交通运输行业是一个庞大的体系,包括铁路、公路、水路、航空和管道等多种运输方式。随着信息化程度的提高,交通运输行业越来越多地依赖于计算机系统和网络进行运营和管理。智能交通、物流信息化等新兴业态不断涌现,极大地提高了运输效率和便利性,与此同时,也带来了前所未有的网络安全挑战。

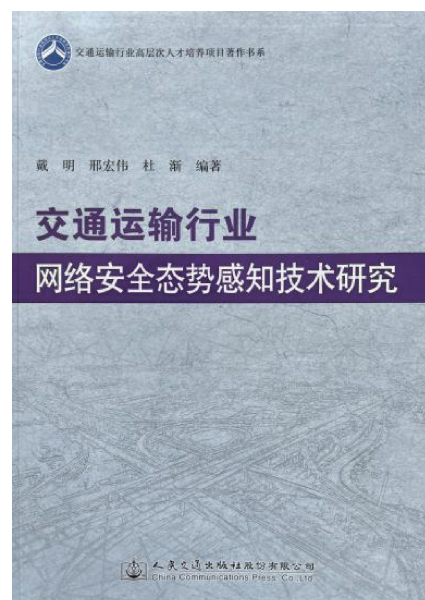
交通运输行业作为国家经济的重要支柱,其网络安全态势的稳定与否直接关系到国家和社会秩序。因此,对交通运输行业网络安全态势感知技术开展研究和分析具有十分重要的现实意义。《交通运输行业网络安全态势感知技术研究》一书介绍了网络安全态势感知在国内外的的发展情况、网络安全态势感知的相关概念及国内国际相关技术标准,全书共分为9个章节。第1章介绍了网络安全发展态势的基本概念和应用情况。第2章阐述了网络态势感知的相关理论知识。第3章分享了网络态势感知发展态势和技术标准,以及我国相关政策、法律法规。第4章介绍交通运输行业网络安全态势感知建设的情况。第5—8章分别研究了网络安全态势感知在公路领域、民航领域、铁路领域及其他行业的具体应用情况。第9章总结了行业网络安全态势感知建设及人才培养。

编者指出,随着交通运输行业信息化的快速发展,网络安全问题日益凸显,而态势感知技术作为一种有效的网络安全管理手段,能够实时监测、分析和预警网络威胁,为交通运输行业的网络安全提供有力保障。编者强调,要提高整个行业的网络安全意识和防护能力,需要加强网络安全管理制度建设,提高网络安全管理人员的专业素质和技能水平。

编者认为,交通运输行业的网络涉及到铁路、公路、航空等多个子领域,一旦发生网络安全事件,可能会影响到整个交通运输系统的正常运行,导致严重的经济损失和社会影响,甚至危及人民群众的生命财产安全。尽管网络安全态势感知技术在交通运输行业中具有广泛的应用前景,但仍存在一些风险和挑战。针对存在的风险和挑战,需要积极采取相应措施来预防。这些措施主要有以下几个方面。首先是建立健全网络安全监测体系。交通运输企业应建立健全网络安全监测体系,实时监测网络中的安全事件。包括对网络流量、日志、设备状态等信息的采集和分析,以及对异常行为的检测和预警。通过网络安全监测体系,企业可以及时发现潜在的安全隐患,为制定防护策略提供依据。其次是加强网络安全技术研发和应用。交通运输企业应加大网络安全技术研发投入,不断提高网络安全防护能力。包括加强密码技术、入侵检测技术、安全审计技术等,并将这些技术应用于实际的网络安全防护中。此外,企业还应关注新兴的网络安全技术和趋势,如人工智能、大数据等,积极探索将其应用于交通运输领域的网络安全防护。再次是建立网络安全应急响应机制。交通运输企业应建立完善的网络安全应急响应机制,确保在发生网络安全事件时能够迅速、有效应对。包括建立应急响应团队,制定应急预案,以及定期进行应急演练。通过应急响应机制,企业可以在网络安全事件发生后迅速采取措施,降低损失。然后是加强网络安全意识和培训。交通运输企业应加强员工的网络安全意识培训,提高员工的网络安全防范能力。如定期开展网络安全知识培训,提高员工对网络安全风险的认识;加强对员工的网络安全行为规范培训,引导员工养成良好的网络安全习惯;加强对员工的网络安全法律法规教育,使员工充分认识到违反网络安全法律法规的严重后果。最后是加强与政府和行业组织的合作。交通运输企业应加强与政府和行业组织的合作,共同应对网络安全风险。包括积极参与政府和行业组织的网络安全工作,如参加网络安全会议、研讨会等;与政府和行业组织共享网络安全信息,提高整个行业的网络安全防护水平,以及在发生网络安全事件时,及时向政府和行业组织报告,寻求支持和帮助。

总之,交通运输企业在面临日益严峻的网络安全风险时,应从网络安全态势感知的角度出发,采取多种措施预防风险。通过建立健全网络安全监测体系、加强网络安全技术研发和应用、建立网络安全应急响应机制、加强网络安全意识和培训以及加强与政府和行业组织的合作,可以有效降低网络安全风险,保障交通运输系统的安全稳定运行。

(徐文硕,许海馨/上海科鑫所商贸服务有限公司)



书名:交通运输行业网络安全态势感知技术研究

编者:戴明,邢宏伟,杜渐

出版社:人民交通出版社股份有限公司

ISBN:9787114180019

出版时间:2022年7月

定价:65元