高速公路收费站网络安全管理面临的挑战与对策研究

文◆安徽皖通高速公路股份有限公司合肥管理处　张　欣

引言

目前，随着高速公路收费站日常运营管理对信息化技术的依赖程度越来越高，网络安全问题也日益凸显。若收费站内没有严谨有效的网络安全防护措施，内部网络一旦被击破，将严重威胁收费站的正常运营。因此，高速公路收费站亟须作出有效应对各种网络威胁的防护策略，为收费站的正常运营保驾护航。基于此，本文对高速公路收费站当前面临的网络安全管理挑战进行了深入研究，并提出应对策略。首先，阐述高速公路收费站网络安全管理面临的威胁和挑战。其次，针对当下网络安全面临的问题提出防护策略。最后，阐述高速公路收费系统网络安全未来发展趋势。

1 高速公路收费站网络安全面临的挑战

随着高速公路业务复杂性的日益增加，收费站面临的网络安全威胁也越来越多，现阶段威胁主要有以下 4 个方面。

（1）外部网络威胁。网络上各类诱导方式层出不穷，黑客攻击手段多样且极具隐匿性，如钓鱼网站、蠕虫病毒等，让人防不胜防，给高速公路收费站的网络安全管理带来了巨大的挑战 [1]。

（2）内部网络结构复杂。通常高速公路管理处辖段内，收费站不止一个，且站与站之间距离较远，每个收费站网络设备众多，收费、监控等内部网络结构复杂，使网络安全管理变得更加困难。

（3）收费设备智慧化程度提升。随着高速公路收费站机电设备智慧化程度的提升，智能化设备所涉及的网络关系节点越来越多，网络关系更为复杂，因此，问题暴露的概率也越来越大。

（4）收费站工作人员网络安全意识薄弱。收费站员工信息化相关知识储备整体偏低，网络安全意识和警惕性不强，随着高速公路各类信息化业务平台的增多，数据泄露的风险也随之增加 [2]。

2 高速公路收费站网络安全管理的应对策略

针对高速公路收费站面临的挑战，目前应对策略可从网络架构、机电设备以及日常管理等层面全方位考虑，分别制定不同的应对策略，确保收费站网络系统的正常运转。

2.1 加强网络层恶意代码防护

据调查，在互联网中恶意代码攻击是目前国内外网络战、信息战最重要的入侵手段之一。在 Internet 安全事件中，因恶意代码攻击而遭受的直接经济损失占比最大。因此，在高速公路收费站网络安全管理中，加强网络恶意代码的防护尤其重要。

（1）流量监测和行为分析。使用流量监测工具与行为分析系统检测异常流量和不寻常的网络行为，分析网络流量和行为模式，有效识别和阻止潜在恶意代码攻击行为，防御恶意代码攻击 [3]。

（2）隔离访问控制。从逻辑上讲，防火墙就像一个隔离器，将防火墙设置在不同网络或网络安全域之间信息唯一出入口的位置，可具备较强的防攻击能力。因此，在收费站内、外网之间设置防火墙实现隔离与

【作者简介】张欣（1989—），女，安徽亳州人，硕士研究生（软件工程），主管工程师，研究方向：交通机电与信息化工程。

访问控制，能够有效监控收费站内网和 Internet 之间的网络活动，从而保证内网安全。

（3）VLAN 隔离技术。VLAN 隔离技术可从逻辑上实现对局域网进行分段，实现对内部子网的物理隔离，解决局域网面临的部分网络安全隐患。另外，还可将安全等级不同、保密要求不同的网段划分到不同的 VLAN 内，限制局域网络安全问题对全局网络造成的影响 [4]。

（4）制定数据备份和恢复计划。制定数据备份和紧急响应计划，防止数据丢失，确保网络系统在受到恶意代码攻击后快速恢复。计划包括定期备份数据、建立灾备中心、进行灾难模拟演练等。

（5）部署网络监控和入侵检测系统。部署网络监控和入侵检测系统，实时监测网络和系统活动，及时发现潜在的异常和攻击行为，使用安全信息和事件管理系统（SIEM）进行日志分析和事件响应。

（6）强化身份验证步骤。实施强大的身份验证措施与合理的访问控制策略，为不同用户分配适当的权限。例如，多因素身份验证和单点登录，确保只有获得授权的人员可以访问敏感信息系统资源。

（7）定期进行网络安全审计。网络安全审计是对网络系统进行全面检测和安全评估的过程，通过审计可以发现网络系统中存在的安全漏洞和薄弱点，及时采取修复措施，使网络系统避免受到黑客攻击 [5]。

2.2 加强服务器安全防护

服务器作为收费站中重要的数据资源存储设备，其对收费站的正常运行起着至关重要的作用。常见的服务器安全防护策略主要有以下 4 种。

（1）加密敏感信息和数据传输。对敏感信息和数据进行加密，确保数据在传输过程中的安全性。使用可靠的加密算法和安全协议，如 SSL/TLS，保护数据在传输过程中的机密性和完整性，防止数据被窃取或篡改 [6]。

（2）安装杀毒软件。在关键服务器安装专业正版杀毒软件，定期升级更新恶意代码库，实时漏洞扫描、安全检测，删除服务器上未经授权的恶意程序，及时发现和修补漏洞，减少潜在攻击面。

（3）加强访问控制。针对收费相关的关键服务器，设置动态密码，定期（一般 1 个月以内）自动修改密码，并注意增加密码的复杂度，密码由管理员统一保管，且设置每个密码只能使用一次，防止密码泄露对服务器安全造成威胁 [7]。

（4）渗透测试。服务器渗透测试是一种评估服务器安全性的测试方法，通过模拟真实攻击的方式，检查服务器系统、网络和应用程序的漏洞和弱点，如数据泄露、服务中断、配置错误、弱密码等，以评估服务器的安全性并提供相应的建议和解决方案。

2.3 提高管理水平

在高速公路收费站日常管理中，技术层面的防护必不可少，但日常管理层面的防护也起到至关重要的作用，日常管理类防护措施主要有以下 3 种。

（1）加强培训。定期开展网络安全培训和教育活动，提高员工的网络安全意识。教授员工识别和预防常见的网络安全威胁的方法，如钓鱼邮件、恶意软件等。加强对密码安全、账号共享和移动设备使用的培训。

（2）完善规章制度。建立完善的网络管理制度，明确网络管理人员的职责，提高网络安全管理责任意识，严格规范各类业务平台的应用管理。例如，使用业务系统时严禁用户使用初始默认密码，严禁将账号转借给他人使用，严禁移动介质在互联网与收费内网之间交叉使用，严禁离岗人员权限不回收等 [8]。

（3）建立应急响应机制。为了做好高速公路收费站网络安全突发事件的防范和应急处理工作，收费站应建立完善的网络安全应急响应机制，提升收费站抵御网络信息及处理安全突发事件的能力和水平，减轻或消除突发网络事件的危害和影响，保证网络的正常运行。一旦发生网络安全事件，迅速响应，有效减轻损失。应急响应机制包含且不限于以下几个方面考虑，即收费内、外网中断的应急处置措施；网站、网页出现非法言论时的紧急处置措施；黑客攻击时的紧急处置措施；计算机网络病毒安全紧急处置措施；办公软件系统遭受破坏性攻击的紧急处置措施；数据库安全紧急处置措施；服务器等关键网络设备故障安全紧急处置措施；自建系统用户账号密码被盗的应急处置措施；专用线路中断时的应急预案等。

3 高速公路收费站网络安全管理的未来发展趋势分析

随着国内外网络环境的不断变化，新的网络威胁和攻击手段不断涌现，高速公路收费站网络安全管理工作也将面临新的挑战。通过预测高速公路收费站网络安全的发展趋势，可以提前采取网络安全防护措施，预防潜在

风险。高速公路收费站网络安全管理的未来发展趋势主要有以下5点。

（1）物联网安全。随着社会的不断进步与物联网技术的广泛应用，各收费站在逐步向智慧一体化收费站发展的同时，也将离不开物联网，因此物联网设备安全将成为网络安全管理的重要方面。高速公路收费站应采取相应的安全防护措施保障物联网设备的安全性，防止物联网设备成为攻击者的入侵点。

（2）人工智能和机器学习。随着科技不断发展，人工智能和机器学习在网络安全中的应用将成为未来主要发展趋势。通过使用人工智能和机器学习，监测和分析行为模式、网络流量和异常活动，实现对网络安全威胁的实时检测，提高对高速公路收费站网络的防御能力，及时发现和应对潜在威胁。

（3）区块链技术应用。区块链技术具备防篡改、多中心化、隐私保护等特点，提供了分散、开放、容错的事务机制。将区块链技术应用于高速公路收费站，不仅有助于提升收费站网络安全管理的透明度和可信度，还可以建立安全的身份认证与访问控制机制，确保只有授权的用户才可以访问收费内网，为收费站提供较好的数据完整性和防篡改能力，确保网络数据信息不受侵害[9]。

（4）网络安全拓展。车联网是新一代网络通信技术和电子、汽车、道路交通等领域深度融合的产业形态。随着未来高速公路智慧化管理系统地研发和推广，今后将实现车与设备、车与云平台、车与车、车与人之间的全方位互联互通、数据共享和智能化管理。在未来发展中，高速公路收费站的网络安全管理工作应拓展到车辆和相关移动设备的安全性，即保护车辆与收费站之间的通信和数据交换，加强车辆系统和移动设备的安全性，防止黑客攻击和恶意软件入侵。

（5）法律法规要求。随着自媒体快速发展，个人信息在互联网的暴露点越来越多。同时，人们对个人信息保护和数据隐私的重视程度逐渐提升，网络安全管理策略应符合更加严格的合规性和法律法规要求。因此，高速公路收费站应根据相关法律法规制定合适的数据信息保护策略、隐私保护措施以及数据删除策略，以确保符合相关法律和监管机构的要求[10]。

结语

高速公路收费站的网络安全管理面临诸多挑战，要想做好网络安全管理工作，就需要从技术、管理等多个方面进行应对。本文对高速公路收费站网络安全存在的漏洞和威胁进行了深入剖析，并从多角度提出了多种防护措施。针对高速公路收费站网络安全管理的未来发展趋势进行了预测，并提供相应的应对参考策略。今后，在高速公路收费站的网络安全管理过程中，应持续关注并适应网络发展趋势，不断提升网络安全管理水平，确保高速公路网络收费系统的安全和稳定运行。

引用

[1] 徐延军,苏鹏.高速公路联网收费网络安全性探讨[J].上海船舶运输科学研究所学报,2008,31(2):98-104.

[2] 任彬彬,丁述庆.基于取消高速公路省界收费站需求的省级联网中心网络安全设计要点[J].大众标准化,2019(12):12-13.

[3] 范平.高速公路联网收费系统网络安全浅析[J].城市建设理论研究(电子版),2023(17):217-219.

[4] 王禹佳,安美谕.高速公路联网收费系统网络安全问题与对策研究[J].交通科技与管理,2023,4(22):15-18.

[5] 李谟珍.浅析湖南取消高速公路省界收费站过程中的网络安全系统[J].中国公路,2021(20):94-95.

[6] 李柳璇子.面向高速公路的智能交通系统网络安全问题研究[J].网络安全和信息化,2023(12):141-143.

[7] 蔡权慧.高速公路联网收费系统网络安全浅析[J].中国交通信息化,2020(4):34-35+103.

[8] 邓力双.高速公路计算机收费网络安全对策研究[J].交通世界,2018(18):170-171.

[9] 吴宏杰.基于区块链的5G物联网数据共享技术[J].科学技术创新,2024(2):135-138.

[10] 张玉晖.宁夏高速公路联网系统网络安全防护的实现策略与基本技术要求[J].中国设备工程,2018(22):210-211.