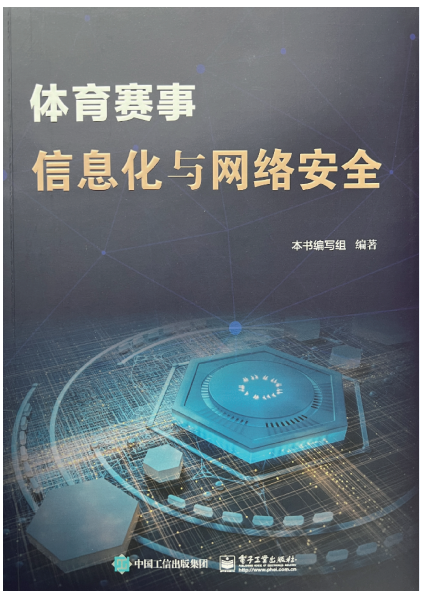
体育赛事组织的网络安全管理策略
——评《体育赛事信息化与网络安全》

数字化时代,大型赛事的运营高度依赖网络系统,涵盖票务管理、实时转播、运动员信息处理等关键环节,其网络安全直接关系赛事公平性、参与者隐私及社会公信力。若体育赛事出现网络安全问题,不仅会造成直接的经济损失,也会对体育文化事业长期发展产生不良影响。因此,强化网络安全管理,是保障赛事顺利进行的前提,更是维护体育精神、守护公众信任的基石,可推动体育赛事产业可持续健康发展。



书名:体育赛事信息化与网络安全
编者:《体育赛事信息化与网络安全》编写组
出版社:电子工业出版社
ISBN:9787121436512
出版时间:2022年6月
定价:78元

体育赛事作为涉及文化、娱乐、经济等多个领域的产业模式,深度依赖媒体运营宣传,信息技术对其组织运营与传播有着重要影响,因此,网络安全是体育赛事组织长远发展的核心要求之一。《体育赛事信息化与网络安全》立足大型体育赛事信息化实践需求,系统构建了涵盖赛事信息化建设与网络安全保障的双重理论框架,是一部兼具技术深度与体系完整性的专著。全书分为2大部分,共14章,逻辑脉络清晰,内容层次分明,体现了“建设-安全”双轮驱动的现代赛事管理理念。第1部分聚焦体育赛事信息化建设,从核心信息系统到基础设施架构展开系统性论述。第1章详细阐释了赛事成绩系统、管理系统、支持系统及主运行中心的架构逻辑与功能协同,揭示了赛事信息流转的底层机制。第2章—第3章深入云计算中心与通信网络的技术实现,系统介绍了从总体架构设计到网络资源池、计算资源池、存储资源池的构建,再到竞赛专网、互联网、转播专网的三网隔离与协同,形成了“云-网-端”一体化的技术支撑体系,为赛事运行提供了弹性可扩展的数字基座。第2部分转向介绍网络安全保障体系,构建了“组织-技术-管理”三维防护框架。第4章—第5章从组织架构与总体安全需求出发,明确提出了网络安全领导小组的职责划分与技术架构设计原则,给出了“顶层规划-技术落地”的闭环。第6章—第9章聚焦场馆网络、云计算中心等关键场景的安全建设,涵盖网络拓扑设计、机房物理安全、虚拟化安全、数据安全监控等具体技术方案,并创新性地提出网络安全管理指挥中心的十大功能模块,实现了威胁感知、溯源分析、指挥调度的全流程覆盖。第10章—第14章从管理体系、检测手段、应急机制、供应链安全到城市遗产思考,形成了“制度-技术-生态”的立体化安全治理体系,特别强调了等级保护定级、渗透测试、红蓝对抗、供应商安全基线等实践工具的应用价值。全书就体育赛事组织的网络安全管理论述全面系统,技术术语严谨,学术逻辑严密,既注重理论框架的构建,又突出实践操作的指导性。通过“信息化-安全化”双线并进的结构设计,不仅系统梳理了体育赛事信息化的技术脉络,更深度挖掘了网络安全保障的内在特征,从而形成从体育赛事组织的建设到防护、从技术到管理的完整知识体系。

作者指出,体育赛事的网络安全管理需突破传统被动防御模式,建立基于赛事全生命周期的动态风险评估机制,将风险识别、评估、防御措施部署与赛事筹备、举办、赛后总结各阶段深度融合,形成闭环管理。赛事筹备阶段,需组建由网络安全专家、赛事运营团队、法律顾问构成的风险评估小组。通过威胁建模技术,针对票务系统、计时计分系统、媒体转播平台、运动员信息管理系统等关键业务场景,系统性梳理潜在攻击路径。例如:票务系统可能面临黄牛利用自动化脚本抢票、伪造二维码入场等风险,需在系统设计阶段引入流量清洗、动态验证码、生物识别验证等技术手段。赛事举办期间,需部署实时威胁情报监测平台,整合开源情报、商业威胁情报、内部日志数据,构建基于大数据分析的动态防御体系。通过机器学习算法异常检测网络流量、用户行为,实现从“已知威胁检测”向“未知威胁预测”的跨越。在大型国际体育赛事中,来自网络的攻击者可能会利用物联

网设备作为跳板发起攻击,如智能摄像头、无线接入点等,为更有效地防御攻击,有必要通过资产指纹识别技术建立设备基线,结合微隔离技术限制设备间非法通信。赛后阶段,负责网络安全工作的部门有必要开展全面的安全审计与经验总结,全面深度复盘安全事件处置过程,从而识别防御体系中的薄弱环节,并优化风险评估模型与防御策略。如针对赛事中出现的钓鱼攻击事件,可分析攻击者所使用的社会工程学手段,并在后续赛事中加强员工安全意识培训,同时,部署邮件网关、沙箱环境等技术预防措施。上述安全管理措施的具体实施需注重技术与管理的双重创新:技术层面要求引入零信任架构理念,对用户、设备、应用实施持续验证与最小权限访问控制;管理层面需建立跨部门协作机制,确保安全团队与赛事运营、技术支持、法律合规等部门保持高效沟通。

笔者认为,体育赛事组织的网络安全管理需建立在对赛事特性的深刻理解之上,不同于常规企业网络,赛事网络具有临时性、高并发性、多部门协同等特点,其安全防护必须展开全维度风险评估。以奥运会为例,从筹备期的场馆建设网络部署、测试赛的系统磨合,到正赛期的票务系统、计时计分系统、媒体直播流的高强度运行,每个阶段都面临独特的安全挑战。风险评估需采用“资产-威胁-漏洞”三维模型。资产识别需覆盖物理设备、数字系统、人员权限 3 个层面,物理设备包括智能场馆的 IoT 传感器、门禁系统、监控摄像头;数字系统涵盖票务平台、计时系统、直播编码器;人员权限涉及志愿者、运动员、媒体记者的临时账号管理。威胁分析需结合历史案例与新兴攻击手法,如 2018 年平昌冬奥会遭遇的“奥林匹克毁灭者”病毒攻击,正是利用赛事网络的临时性特点,通过钓鱼邮件快速扩散。漏洞评估则需采用“红队演练+蓝队防御”模式,由专业团队模拟黑客攻击路径,发现系统薄弱点。动态防御体系需具备“自适应、可扩展、可回溯”3 大特性。自适应性体现在安全策略能根据赛事阶段自动调整,筹备期重点防范供应链攻击,正赛期强化分布式拒绝服务防护,赛后需确保数据归档安全。可扩展性要求系统能应对突发流量,如世界杯开幕式时的票务系统瞬间访问量激增,需通过弹性云架构实现快速扩容。可回溯性则依赖完整的日志审计系统,确保任何操作都有迹可循,便于事后分析。具体实施中,需建立“三纵三横”的防御矩阵。纵向按层级分为终端安全、网络边界安全、云端安全;横向按功能分为访问控制、数据加密、行为分析。如终端安全需部署智能杀毒软件,实时监测异常进程;网络边界安全需设置防火墙与入侵检测系统,防止未授权访问;云端安全需采用零信任架构,确保每次访问都经过多因素认证。数据加密需贯穿“传输-存储-使用”全流程,如直播流采用 AES-256 加密,票务信息使用端到端加密传输。行为分析引入 AI 驱动的异常检测系统,通过机器学习识别正常行为基线,快速发现异常登录、数据异常下载等可疑操作。

体育赛事组织的网络安全管理需以系统性风险评估为基石,构建动态防御体系。不同于企业的静态防御模式,赛事场景具有时间敏感性、人群聚集性、媒体曝光度高等特殊属性,要求安全策略必须覆盖物理层、网络层、数据层、应用层及人员层 5 大维度。在物理层防护方面,需对赛事场馆的服务器机房、网络设备间实施严格的门禁管控与视频监控,部署环境监测系统实时监控温湿度、烟雾等参数。网络层防御需构建多层次纵深防御体系,外网边界应部署下一代防火墙实现流量清洗,通过入侵防御系统/入侵检测系统实时监测异常流量模式;在内部网络划分方面,采用微隔离技术将赛事运营、媒体转播、观众服务等不同业务域进行逻辑隔离。数据层保护需建立分类分级管理制度,赛事涉及的个人信息、财务数据、比赛成绩等敏感信息必须采用 AES-256 加密存储,传输过程强制使用 TLS 1.3 协议。特别需要关注第三方供应商的数据访问权限管理,通过建立数据访问白名单与操作审计日志,实现全流程可追溯。应用层安全需贯穿开发、测试、部署全生命周期,采用 DevSecOps 理念将安全测试嵌入开发流水线,通过静态代码分析、动态渗透测试、交互式应用安全测试等手段提前发现漏洞。针对赛事票务系统的高并发特性,需进行压力测试与混沌工程演练,确保在流量洪峰下仍能保持系统韧性。

总之,体育赛事的网络安全管理是一场没有终点的马拉松,既需要技术创新的持续领跑,也离不开管理智慧的稳健护航。从系统架构的精密设计到风险防控的动态演进,从智能监控的实时响应到安全文化的深层渗透,每一步都需凝聚共识、形成合力。未来,随着技术迭代与场景拓展,网络安全管理将更深度融入赛事治理流程,成为守护公平、信任与价值的核心屏障。唯有将“安全”二字刻入赛事基因,方能在数字浪潮中行稳致远,让体育精神在安全可信的数字空间中绽放更璀璨的光芒。

(林羽姗/福州外语外贸学院教育学院/讲师)