计算机监控系统综合安全管理平台建设探讨

张 宁[1],张昊鹏[2],张 磊[1]

(1.山东省水利综合事业服务中心,山东 济南 250014;2.山东省调水工程运行维护中心烟台分中心,山东 烟台 264000)

【摘 要】文章主要分析了胶东调水计算机监控系统结构及其网络安全现状,提出了通过构建计算机监控系统综合安全管理平台,实现计算机监控系统安全监控、安全管理、安全运营,实时掌握计算机监控系统整体业务运行状况与安全情况,及时发现网络安全风险,有效保护网络运行安全,完善安全管理相关规章制度及网络安全相关应急预案,提高网络安全应急响应能力和协同工作效率。

【关键词】监控系统;网络安全;综合安全管理平台

【中图分类号】F426.91 【文献标志码】A 【文章编号】1009-6159(2025)-05-0026-03

Discussion on the Construction of a Comprehensive Security Management Platform for Computer Monitoring Systems

ZHANG Ning[1], ZHANG Haopeng[2], ZHANG Lei[1]

(1. Water Resources Comprehensive Development Center of Shandong Province, Jinan, Shandong 250014, China;
2. Yantai Branch Center, Water Diversion Project Operation and Maintenance Center of Shandong Province, Yantai, Shandong 264000, China)

Abstract: This paper analyzes the structure of the computer monitoring system for Water Diversion to Jiaodong Area and the current situation of its network security. It proposes that by constructing a comprehensive security management platform for the computer monitoring system, the security monitoring, security management, and security operation of the computer monitoring system can be realized. This allows for real-time grasp of the overall business operation status and security situation of the computer monitoring system, timely detection of network security risks, effective protection of network operation security, improvement of relevant rules and regulations for security management and emergency plans related to network security, and enhancement of network security emergency response capabilities and collaborative work efficiency.

Key words: Computer monitoring system; Network security; Comprehensive security management platform

1 胶东调水网络安全管理现状

计算机监控系统作为胶东调水自动化调度系统中的关键子系统,是胶东调水工程实现优化调度、提高运行和管理自动化水平的基础。胶东调水计算机监控系统是在通信传输和计算机网络建设基础上,采用先进成熟的计算机、自动控制和传感器技术,通过现地监测、控制等自动化设施建设,实现对胶东调水工程的13座调水梯级泵站、95处闸站、46处阀站控制站等建筑物监测点的运行信息和运行状态的远程监测和控制。整个计算机监控系统从管理层级角度分为三级架构:监控中心(调度中心与备调中心),监控泵站分中心(部署在13个泵站),泵站、闸站与阀站现地。系统设计采用扁平结构,从软件架构上采用二级(中心、泵站分中心)分布式方式部署,6个市分局及部分县管理站采用客户端进行监控。

省中心计算机监控系统部署了网闸、工业防火墙、IPS等网络安全设备,网络安全防护设备及手段较为完善,具备边界防护、访问控制、入侵防范、安全审计等防护功能。但依据等保2.0国家标准,尚缺乏一体化综合安全管理平台,对整个计

收稿日期:2025-02-29

作者简介:张宁(1978—),男,工程师

算机监控系统日志、操作、网络设备和安全设备进行统一管理,不能实时掌握计算机监控系统整体业务运行状况与安全情况。网络安全管理制度不完善,需要系统的、体系化的进行制度建设。员工缺乏培训,对网络安全的基本知识掌握有限,缺乏必要的网络安全防护相关知识。相应网络安全应急预案缺乏,没有定期进行网络安全应急演练工作。网络安全运维工作没有科学的管理与评价手段,对维护人员的权限、准入的监控与管理缺乏行之有效的技术手段。

2 综合安全管理平台建设思路

综合安全管理平台应能实现对计算机监控系统资产、业务应用、制度及执行流程、运维等进行全面统一管理,具备安全监控、安全管理、安全运营等功能,实现计算机监控系统设备、人员、制度、应急、运维、培训等综合安全管理,形成多层次、多维度的防御体系。简化管理和操作流程,提供统一界面和工作流程。实时监测和检测威胁,快速识别和应对攻击。提供统一视图和报告功能,帮助了解系统网络安全状况。并具备跨平台和集成性,提高安全管理效率。

3 综合安全管理平台功能

3.1 安全监控功能

1)资产统一管理。通过安全管理平台资产自动发现功能,自动发现在网设备资产,获取设备类型,系统版本型号,mac 地址,ip 地址,以及对外提供的服务端口等数据,对计算机监控系统所有的 IT 资产进行梳理、排查与摸底,并将在网 IT 设备全面纳入管理。建立资产档案库,详细记录资产上线到报废过程中所有的管理、变更、配置等信息,实现配置项变更管理流程,并对资产生命周期中的所有配置变更,提供记录功能,记录变更的申请和处理的全历史过程,对资产全生命周期进行管理。

2)网络结构拓扑建立。建立计算机监控系统网络拓扑图与业务拓扑图,直观展示业务系统和各设备(网络安全设备、服务器、虚拟网络、虚拟机等 IT 资源)的运行情况,包括设备之间的网络链接、流量的动态走向、链路颜色区别和负载情况,支持链路状态呈现和告警定位,显示内部链路及出入口链路的状况及流量信息。

3)日志统一审计。对计算机监控系统各种应用程序、网络设备和安全设备生成的日志进行集中管理和审计,从多维度对审计结果进行统计分析,反映计算机监控系统运行状态。通过对日志进行统一审计,全面实现事件可追溯性和合规性监控。

4)资源监控与告警。对计算资源、网络设备、应用程序等关键设备和组件进行实时监控,监控内容包括 CPU 利用率、内存利用率、存储器信息、网口信息、进程信息等,并在异常情况发生时生成告警。通过资源监控与告警,实现对关键资源的实时监控和异常检测,及时发现和解决问题,提高系统的稳定性和可用性。同时,告警通知可以帮助技术人员快速响应并处理问题,减少系统故障对业务的影响。

5)全网统一监控。建立整个网络环境的统一监控,通过网络拓扑图和资源管理、实时流量监测、事件和日志管理、故障和性能监控、告警和报告以及远程管理和访问控制等措施,实现对网络的实时监测、管理和分析。将连通性中断、运行监测指标超过阈值、网络病毒攻击、人员误操作等告警进行统计和分类,并进行统一展示。

3.2 安全管理功能

1)安全事件的采集管理。通过建立健全安全事件采集机制,及时发现、记录和上报网络安全事件,为及早采取相应的应对措施提供重要支持。安全管理平台通过监测和记录网络设备、信息系统与安全设备的运行状态和异常情况,实时收集安全事件的相关信息,主要包括设备与系统的业务连续性、异常访问、未经授权的操作、恶意软件的侵入以及其他潜在的安全威胁等。通过有效的安全事件采集管理功能,可以快速、准确地获取安全事件的信息,并及时采取必要的措施来应对和解决问题,有助于减少潜在的安全风险,提升整体的网络安全能力和防护水平。

2)安全处置的统一管理。安全处置的统一管理是确保计算机监控系统网络安全的关键环节,涉及对安全事件的及时响应、有效处理和持续监控,以保障计算机监控系统的正常运行和安全性。统一管理建立完善的安全处置入口,通过统一管理安全处置工作,能够加强对安全事件的管理和监控,提高应对能力和处置效率,确保计算

机系统的安全稳定运行，有效应对各类安全风险和威胁，保障计算机监控系统的安全运行。

3）网络安全合规任务下发与反馈。通过安全管理平台可向员工下发密码强度设置、网络安全保密、网络安全培训学习等网络安全合规任务，并收集和反馈任务的执行情况，确保网络安全合规工作的有效实施和监督。

4）安全管理制度建设与落实情况跟踪。安全管理平台具备网络安全管理体系建设功能，具有相关管理制度、管理机构、管理人员、系统建设、安全运维等制度模板，可根据实际情况修改。并将相关网络安全管理制度电子化、策略化、任务化，确保制度落地执行并收集相关制度落实情况。

3.3 安全运营功能

1）网络安全应急预案管理。安全管理平台具有网络安全应急预案与应急演练制定、管理和执行功能，提供网络安全应急预案模板，协助进行网络安全预案建设及预案管理。

2）应急演练管理。网络安全应急演练，可提高在网络安全事件发生时的应急响应能力和协同工作效率。安全管理平台提供应急演练计划制定模板，应急演练计划模板包括目标范围、安全团队和职责、事件分类和级别、网络监测和报警、风险评估和预警、事件响应流程、数据备份和恢复等内容，并详实记录应急演练的过程。

3）安全培训管理。安全管理平台内置网络安全知识库，集中存储和管理网络安全相关知识资料，可提供全面的安全培训，增强员工对安全威胁的认识，提高应对和防范网络安全事件的能力。培训教材包括网络安全概念和基础知识、网络安全风险管理、网络安全防护技术等等，为员工提供易于访问和查阅的网络安全知识资源，帮助员工提高网络安全意识和知识水平。

4）安全人员管理。通过建立人员工作报告和绩效管理办法，收集和分析与 IT 服务相关的数据和指标，例如服务请求数量、问题解决时间、客户满意度等。生成报告和仪表板，监控和评估 IT 服务效果和绩效。根据报告和指标，评估 IT 服务的效果和质量。发现问题和瓶颈，并采取适当的措施改进服务流程和操作。提供绩效报告给相关人员，以便了解 IT 服务的表现和价值。

5）报表建设。安全报表是用于汇报和展示安全状况、安全控制措施的实施情况以及安全事件和威胁的发生情况。包括安全漏洞报表；安全事件报表：记录已发生的安全事件；安全控制评估报表：评估和审查安全控制措施的有效性和符合性；安全风险评估报表：对整体的计算机监控系统进行风险评估，识别和分析潜在的安全风险和威胁，并提供相应的风险解决措施和建议；安全合规性报表：根据适用的法律法规和行业标准，评估安全措施是否符合合规要求，并提供合规性状况和改进建议；安全意识培训报表：记录安全意识培训的实施情况和效果评估。安全性能指标报表：收集和分析与安全性能相关的指标和数据，以评估和改进安全运营的效率和效果。

6）网络安全运维流程规范化。安全管理平台内置网络安全运维流程管理，提供故障处理、报修流程、制度管理、运维工单等多种模板，也可根据实际情况进行流程自定义。通过规范化运维流程，可确保安全运维按照既定的步骤和标准进行，减少错误与风险、人为失误、提升运维效果。

4 结 语

胶东调水综合安全管理平台基于计算机监控系统的业务应用特性，结合系统网络结构、业务流程和内容，建立综合安全防护体系，实现网络中病毒、入侵、违规操作等安全风险的准确发现与精准控制，实时掌握网络中存在的各种安全风险，有助于风险预警与处置，有效的保护网络运行的安全。有助于安全管理机构、管理人员、安全运维等相关管理制度的建立健全，并保障规章制度的落实和执行。有助于完善网络安全相关应急预案，制定网络安全演练计划，提高网络安全应急响应能力和协同工作效率。有助于安全运维标准化、规范化，减少人为失误，提高运维效率。

参考文献

[1] 国家市场监督管理总局. 网络安全等级保护测评要求：GBT28448-2019[S].北京：中国标准出版社，2019.

[2] 中华人民共和国国家质量监督检验检疫总局.工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序：GB/T 33007-2016[S].北京：中国标准出版社，2016.

[3] 国家市场监督管理总局.信息安全技术 网络安全等级保护基本要求 GBT22239-2019，北京：中国标准出版社，2019.

（责任编辑 赵其芬）