水电水利
Hydropower and Water Resources
第 8 卷◆第 8 期◆版本 1.0◆2024 年
文章类型：论文|刊号（ISSN）：2529-7821 /（中图刊号）：868GL002

水利工程数字化进程中网络安全风险与防御

邓天麒
新疆水发水务集团有限公司
DOI:10.12238/hwr.v8i8.5660

[摘　要] 随着水利行业向数字化、智能化转型的加速,网络安全问题日益凸显。本文深入分析了水利数字化过程中面临的网络安全挑战,包括数据泄露、系统入侵、新技术应用风险等,并据此提出了一系列针对性的防御策略,旨在构建全面、高效的网络安全防护体系,保障水利行业数字化转型的顺利进行。
[关键词] 水利工程；数字化进程；安全挑战；防御策略
中图分类号：TV　文献标识码：A

Digitalization in Water Conservancy Projects: Cybersecurity Risks and Defenses

Tianqi Deng
Xinjiang Shuifa Water Affairs Group Co., Ltd

[Abstract] With the accelerated digital and intelligent transformation of the water conservancy industry, cybersecurity issues have become increasingly prominent. This paper delves into the cybersecurity challenges faced during the digitization process of water conservancy projects, encompassing data breaches, system intrusions, and risks associated with the application of new technologies. Based on these analyses, a series of targeted defensive strategies are proposed, aiming to establish a comprehensive and efficient cybersecurity protection system to ensure the smooth progress of the digital transformation in the water conservancy industry.
[Key words] water conservancy projects; digitalization process; security challenges; defensive strategies

引言

水利行业作为国家基础设施的重要组成部分,其数字化转型对于提升水资源管理效率、增强防洪抗旱能力具有重要意义。然而,在享受数字化带来的便利与效益的同时,水利行业也面临着前所未有的网络安全威胁。这些威胁不仅可能破坏水利系统的正常运行,还可能对国家安全和社会稳定造成严重影响。因此,深入探讨水利数字化进程中的网络安全挑战与防御策略,对于保障水利行业的健康发展具有重要意义。

1 水利工程数字化进程中网络安全的重要性

水利工程数字化是指将传统的水利工程管理与现代信息技术相结合,通过数字化手段对水利工程进行规划、设计、施工、运行和维护等全生命周期的管理。这一过程涉及到多种高新技术,如BIM(建筑信息模型)、GIS(地理信息系统)、遥感技术、全球定位系统等,以实现水利工程的可视化、智能化和精细化管理。在水利工程数字化进程中,网络安全的重要性不言而喻。具体如下：(1)保障数据安全。水利工程数字化过程中产生了大量的敏感数据,包括水文监测数据、工程运行数据、用户信息等。这些数据对于水利工程的运行管理和决策制定至关重要。一旦这些数据被非法获取或篡改,将可能导致严重的后果,如工程安全受到威胁、决策失误等。(2)确保系统稳定运行。水利工程数字化系统是实现水利工程自动化、智能化管理的关键。一旦系统遭受网络攻击,如病毒入侵、拒绝服务攻击等,将导致系统瘫痪或运行异常,严重影响水利工程的正常运行。(3)防范潜在风险。随着网络技术的不断发展,新的网络安全威胁层出不穷。对于水利工程数字化系统而言,必须时刻保持警惕,防范潜在的网络安全风险。通过建立完善的网络安全防护体系,包括防火墙、入侵检测系统、安全审计系统等,可以有效降低网络安全风险,保障水利工程数字化系统的安全稳定运行。(4)促进数字化转型。网络安全是水利工程数字化转型的重要保障。只有确保网络安全,才能消除转型过程中的顾虑和障碍,推动数字化转型的顺利进行。同时,随着数字化转型的深入,水利工程将实现更加高效、智能的管理和决策。这将有助于提升水利工程的整体效能,为社会经济发展提供更加坚实的水利支撑。

2 水利数字化面临的网络安全威胁

新疆地域辽阔,水资源分布不均,水利工程建设与管理任务繁重。近年来,新疆水利行业积极响应国家号召,加速推进数字化进程,旨在通过现代信息技术提升水资源管理效率、增强防洪抗旱能力。然而,在享受数字化带来的便利与效益的同时,新疆水利行业也面临着更为复杂和严峻的网络安全挑战。这些挑战

文章类型：论文|刊号（ISSN）：2529-7821 /（中图刊号）：868GL002

不仅关乎水利系统的稳定运行,更直接影响到新疆的经济社会发展与生态安全。

2.1外部网络攻击

随着网络技术的不断发展,黑客攻击手段日益多样化和复杂化。水利数字化系统作为重要的基础设施,往往成为黑客攻击的目标。一旦系统被入侵,黑客可能通过篡改数据、破坏系统等方式,对水利工程的正常运行造成严重影响。具体来讲：(1)恶意软件攻击。黑客可能通过向水利工程数字化系统中注入病毒、木马、蠕虫等恶意软件,实现对系统的非法控制或数据窃取。这些恶意软件可能导致系统瘫痪、数据泄露或信息篡改等严重后果。(2)DDoS攻击。分布式拒绝服务攻击(DDoS)是一种通过控制大量计算机或网络设备向目标系统发送大量请求,导致系统资源耗尽而无法正常响应的攻击方式。对于水利工程数字化系统而言,DDoS攻击可能导致系统瘫痪,影响水利工程的正常运行。(3)社会工程学攻击：黑客可能通过冒充系统员工、合作单位或伪造电子邮件、短信等方式,获取敏感信息或系统访问权限,进而对系统进行攻击或破坏。

2.2内部安全漏洞

在水利工程数字化进程中,内部安全漏洞是一个不容忽视的问题,它们可能源自技术、配置及人为因素等多个方面。(1)技术更新滞后。水利工程的建设往往涉及庞大的规模和复杂的系统,因此其建设周期相对较长。在这个过程中,技术发展迅速,新的安全威胁和漏洞不断被发现。然而,由于项目周期长、资金限制或管理疏忽等原因,部分系统可能长时间未进行必要的更新或升级。这些老旧系统往往存在已知的、已被公开的安全漏洞,攻击者可以轻易利用这些漏洞来入侵系统、窃取数据或破坏系统正常运行。(2)配置不当。系统配置是确保系统安全性的关键环节之一。然而,在实际操作中,由于配置错误或疏忽,可能导致系统存在安全隐患。例如,未启用必要的安全策略(如访问控制、数据加密等)、未设置强密码、未限制不必要的网络访问等,都可能为攻击者提供可乘之机。这些配置不当的问题可能使系统面临数据泄露、非法访问等风险。(3)安全意识薄弱。内部员工是系统安全的第一道防线。然而,由于安全意识不足或培训不到位等原因,员工可能无意中泄露敏感信息或执行不安全的操作。例如,随意分享密码、点击恶意链接、使用不安全的设备访问系统等行为都可能给系统带来安全隐患。此外,员工还可能对安全策略产生抵触情绪或忽视安全提示信息,进一步增加系统的安全风险。

2.3数据安全挑战

水利数字化过程中,海量数据的收集、处理、存储和传输成为常态。这些数据中包含了大量敏感信息,如水文监测数据、工程运行数据等。一旦这些数据被非法获取或滥用,将可能导致严重的后果。(1)数据泄露风险。在水利工程数字化进程中,大量敏感数据需要在不同系统、不同部门之间传输,如水文监测数据、工程运行数据、设备状态信息等。这些数据对于水利工程的安全运行至关重要,一旦在传输过程中被未授权的第三方截获或泄露,将带来以下严重后果。例如：敏感数据的泄露可能暴露水利工程的脆弱点,为恶意攻击者提供可乘之机,进一步威胁水利工程的安全；泄露的数据可能包含商业机密或敏感信息,如工程成本、维护计划等,这些信息一旦落入竞争对手或不法分子手中,将给水利工程带来直接的经济损失；水利工程的稳定运行直接关系到社会公共利益和民生福祉。数据泄露可能引发公众恐慌,损害政府公信力,甚至引发社会不稳定因素。(2)数据篡改风险。攻击者可能通过技术手段对传输中的数据或存储中的数据进行篡改,以达到干扰水利工程正常运行或误导决策的目的。基于篡改后的数据进行决策,可能导致水利工程调度失误、资源分配不合理等后果,进而影响工程的整体效益和安全；篡改控制指令可能导致水利工程中的设备异常运行,甚至造成设备损坏,增加维护成本和风险。数据篡改可能破坏数据的真实性和可信度,导致用户对水利工程的信任度降低,影响工程的正常运行和管理。(3)数据丢失风险。数据丢失是数据传输与存储过程中常见的风险之一。由于系统故障、人为错误或自然灾害等原因,重要数据可能面临丢失的风险。关键数据的丢失可能导致水利工程业务中断,影响工程的正常运行和管理；数据丢失后,为了恢复业务,需要投入大量的人力、物力和财力进行数据恢复工作,增加工程成本；在某些情况下,数据丢失可能涉及法律责任问题,如违反数据保护法规、泄露用户隐私等,给水利工程带来法律风险和声誉损失。

2.4新技术应用风险

随着物联网、云计算、大数据等新技术在水利工程数字化进程中的广泛应用,也带来了新的安全挑战。例如,物联网设备的激增带来了新的安全问题；云计算的普及使得企业越来越依赖少数云服务商,一旦出现问题将影响巨大。

(1)云计算的安全风险。云计算的普及使得企业越来越依赖少数云服务商。然而,这种集中化的数据存储方式也带来了风险。一旦云服务商的数据中心遭受攻击或出现故障,将影响大量企业的业务运行,包括水利工程；云计算服务的稳定性和可用性对水利工程至关重要。如果云服务商的服务中断或性能下降,将直接影响水利工程的正常运行和管理；在云计算环境中,不同用户的数据可能存储在同一个物理服务器上。如果云服务商的数据隔离措施不到位,可能导致数据泄露或被非法访问。(2)大数据的安全风险。大数据技术的应用使得水利工程能够收集和分析大量敏感数据。然而,这些数据在处理和存储过程中如果未采取足够的安全措施,可能导致隐私泄露；大数据的准确性和完整性对水利工程的决策至关重要。如果数据质量不高,存在错误或不一致等问题,将影响决策的准确性和可靠性；大数据的广泛应用也带来了数据滥用的风险。如果敏感数据被未经授权的第三方获取并利用,将对水利工程的安全和稳定造成威胁。

3 水利数字化网络安全防御策略

3.1强化数据安全管理

(1)建立健全的数据安全管理制度。制定详细的数据安全管理制度,明确数据的分类分级标准,对不同级别的数据实施不同

的安全保护策略。实施严格的数据访问控制，确保只有经过授权的人员才能访问敏感数据。采用数据加密技术，对敏感数据进行加密存储和传输，防止数据在传输和存储过程中被窃取或篡改。(2)加强数据备份和恢复机制建设。建立定期数据备份制度，确保重要数据的完整性和可恢复性。配备专业的数据恢复设备和工具，以便在数据丢失或损坏时能够迅速恢复。

3.2提升系统安全防护能力

(1)采用先进的网络安全技术和设备。部署防火墙、入侵检测系统、安全审计系统等网络安全设备和系统，构建多层次的防御体系。加强对系统漏洞的监测和修复工作，利用自动化工具和人工审核相结合的方式，及时发现并修复系统漏洞。及时更新安全补丁和防护措施，确保系统始终保持在最新的安全状态。(2)建立应急响应机制。制定详细的应急响应预案，明确应急响应流程和责任分工。定期组织应急演练，提高应急响应团队的协同作战能力和应急处置效率。在遭受攻击时，能够迅速启动应急响应机制，采取有效措施遏制攻击并恢复系统正常运行。

3.3加强供应链安全管理

(1)对供应商进行严格的资质审查和安全管理要求。在选择供应商时，不仅要考虑其技术实力和服务水平，还要对其安全能力和保障措施进行严格审查。要求供应商提供详细的安全管理制度和措施，并签署保密协议和安全责任书。(2)加强采购过程中的安全性评估和测试。在采购网络设备和软件时，要进行严格的安全性评估和测试工作，确保设备和软件不含有恶意代码和后门等安全问题。对于关键设备和软件，可以邀请第三方安全机构进行独立的安全评估和测试。

3.4提升人员安全意识与技能

(1)加强网络安全培训和教育工作。定期组织网络安全知识讲座和培训活动，提高水利从业人员的网络安全意识和技能水平。培训内容应包括网络安全基础知识、常见网络攻击手段及防御方法、应急响应流程等。(2)建立健全的网络安全责任制和奖惩机制。将网络安全工作纳入员工绩效考核体系，明确网络安全责任人和职责范围。对在网络安全工作中表现突出的员工给予表彰和奖励；对违反网络安全规定的行为进行严肃处理并追究相关责任。

3.5加强跨部门协作与信息共享

(1)建立网络安全信息共享平台和工作机制。搭建跨部门的网络安全信息共享平台，实现网络安全威胁情报的及时共享和传递。建立定期的信息交流和沟通机制，确保各部门在网络安全工作中能够协同作战、形成合力。(2)加强与相关机构和企业的合作与交流：积极参与国家网络安全相关机构和组织的活动，及时了解网络安全领域的最新动态和技术趋势。加强与同行业企业的合作与交流工作，共同应对网络安全挑战并分享成功经验。

4 结束语

水利数字化进程中的网络安全挑战不容忽视。通过强化数据安全管理、提升系统安全防护能力、加强供应链安全管理、提升人员安全意识与技能以及加强跨部门协作与信息共享等措施的实施，可以构建全面、高效的网络安全防护体系，为水利行业的数字化转型提供有力保障。未来，随着技术的不断进步和应用的不断深化，水利数字化网络安全工作将面临更多新的挑战和机遇。因此，我们需要持续关注网络安全领域的发展动态和技术趋势，不断创新和完善网络安全防护策略和方法手段，为水利行业的健康发展保驾护航。

[参考文献]

[1]刘艳林,文恒.地理信息系统及其在水利中的应用[J].内蒙古科技与经济,2007(17):86-88.

[2]沈宏平,田明云.计算机网络技术在水利工程管理中的应用[J].江苏水利,2004,(10):27-29.

[3]蒲果.计算机网络技术在水利水电工程中的应用[J].水利水电施工,2010,(3):88-90.

作者简介：

邓天麒(1994--),男,汉族,新疆乌鲁木齐人,大学本科,初级工程师,研究方向：水利工程网络安全。