水利网络安全监测与预警体系分析

张浩翔
河北水务有限公司　河北　石家庄　050000

摘　要：随着信息技术的快速发展，水利行业正逐步迈向信息化、智能化。然而，水利网络安全问题也日益凸显，成为制约水利信息化发展的关键因素。本文深入分析了水利网络安全监测与预警体系面临的问题，并提出了相应的完善措施。通过构建全面、高效的水利网络安全监测与预警体系，可以有效提升水利行业的网络安全防护能力，确保水利信息化建设的顺利进行。

关键词：水利；网络安全；监测；预警体系

引言

水利行业作为国民经济的重要组成部分，其信息化建设对于提高水资源管理效率、保障防洪安全等具有重要意义。然而，随着信息技术的广泛应用，水利网络安全问题也日益突出。网络攻击、信息泄露等事件频发，严重威胁着水利行业的安全稳定。因此，构建水利网络安全监测与预警体系，及时发现并应对网络安全威胁，已成为水利信息化建设的迫切需求。

1 水利网络面临的安全威胁

1.1 网络攻击日益猖獗

目前，带有国家背景的网络攻击尤为引人注目，它们不仅瞄准了商业机密、敏感数据，更将触角伸向了核弹级武器研发信息的窃取与泄露，这一系列行动如同在网络世界中引爆了一颗颗隐形的核弹，威胁着全球的网络安全与和平稳定。2017年5月12日，一个名为WannaCrypt（又称“永恒之蓝”）的勒索蠕虫病毒横空出世，这一事件标志着美国国家安全局（NSA）网络军火库中的武器首次被非法泄露并用于全球范围内的民用攻击。短短一天多的时间里，WannaCrypt病毒如野火燎原，迅速席卷了全球近百个国家，超过10万家企业和公共组织不幸中招，数万台电脑系统陷入瘫痪状态，其影响之广、速度之快，令人咋舌[1]。从象牙塔内的高等学府到繁忙的火车站，从便捷的自助服务终端到承载着千家万户通信需求的邮政系统，从能源供应的关键节点加油站到医院这一生命守护之地，再到政府机构的日常运作，无一幸免于这场网络风暴的侵袭。在我国，这场危机同样来势汹汹，各地区的高校、公共服务机构均报告了感染情况，显示出网络攻击无孔不入、跨越国界的恐怖威力。尤为值得警惕的是，水利部作为关乎国计民生的重要部门，也未能在这场网络风暴中独善其身。据统计，仅在今年4月份，水利部机关就遭受了上百万次的网络攻击尝试，其中针对水利部网站的入侵攻击占比高达45.79%，紧随其后的是拒绝服务攻击，占比38.59%。这些攻击不仅试图非法侵入系统，窃取敏感信息，还试图通过瘫痪服务来干扰水利设施的正常运行，其潜在后果不堪设想。面对如此高频次、高强度的网络武器级攻击，任何一个行业或部门单独作战，都显得力不从心，难以有效抵御。

1.2 安全措施落实不到位

在当前这个数字化时代，网络安全已成为各行各业不可忽视的重大议题。尽管大多数单位和组织已经意识到了网络安全的重要性，并为此制定了一系列网络安全管理制度，然而在实际操作中，这些制度的执行情况却不容乐观，存在着落实不到位的问题，这不仅削弱了安全防护的效果，也为潜在的安全风险埋下了伏笔。理论上，为了构建稳固的网络安全防线，许多单位都投入了大量资源，部署了包括防火墙、网络安全审计系统、入侵检测系统在内的多种安全防护设备。这些技术手段在一定程度上增强了网络环境的防御能力，为数据的安全传输和存储提供了技术支持。然而，令人遗憾的是，这些安全防护设备并没有形成一个完整、协同的安全体系。究其原因，一方面在于安全策略的制定缺乏科学性和细致性，往往过于笼统或片面，难以全面覆盖各种潜在的安全威胁；另一方面，则在于安全策略的执行力度不足，导致即使有先进的技术手段也难以充分发挥其应有的作用。更为严重的是，许多单位在网络安全工作中存在着重建设轻管理的现象。他们往往过于关注安全防护设备的采购和部署，却忽视了后续的维护和管理工作。这种短视的做法不仅使得安全防护设备在长期使用中逐渐失去效用，还可能因为缺乏必要的更新和升级而暴露出新的安全漏洞。

1.3 安全漏洞处置不及时

在当今这个高度信息化的社会，网络安全已成为各行各业不可忽视的关键要素。为了确保系统的安全稳定运行，大部分单位都采取了定期漏洞扫描这一基础且重要的安全措施。但是，尽管这一做法在理论上能够及时发现并定位系统中的安全漏洞，但由于多种实际因素的制约，漏洞扫描的后续处置工作却往往不尽如人意，成为历年网络安全检查中一个较为突出的问题。具体而言，尽管大部分单位都能够按照既定的计划进行漏洞扫描，但受限于技术人员匮乏、技术力量薄弱等瓶颈问题，这些单位在扫描完成后往往只能停留在生成安全检测报告的层面。这份报告虽然详细列出了系统中存在的安全漏洞及其潜在风险，但由于缺乏足够的技术支持和人员配备，这些漏洞往往无法得到及时的修复和整改。这就好比一个人定期体检后发现了身体上的问题，但由于种种原因没有及时就医治疗，导致问题日益严重，最终影响到整体健康[2]。并且，系统长期带病运行，安全隐患层出不穷，这一现状不仅削弱了系统的防御能力，也为黑客攻击提供了可乘之机。一些原本可以通过及时修复漏洞来避免的安全事件，由于处置不及时而演变成了严重的安全事故。这些事故不仅给单位带来了经济损失和声誉损害，还可能对社会的稳定和安全造成威胁。

2 构建水利网络安全检测与预警体系的措施

2.1 加强水利网络安全检测

在技术层面，水利部门积极引入先进的网络安全检测技术，不断提升网络安全监测的精准度和效率。同时，为了拓宽信息来源，增强网络安全防护的全面性，水利部门还加强了与外部技术部门的交流合作，通过信息共享和协同作战，构建了一套完整合理的网络信息处理系统。这一系统能够高效整合各类网络安全信息，实现信息的快速传递和有效分析，为水利网络安全的科学决策提供了有力支持。在加强内部建设的同时，水利部门还积极寻求外部合作，与国家中央网信办、公安部门以及工信部门等建立了紧密的合作关系。这些合作不仅为水利部门提供了丰富的网络安全资源和专业指导，还促进了部门间的高效联动，形成了网络安全防护的强大合力[3]。通过整合各方优势资源，水利部门能够更有效地应对网络安全挑战，提升水利网络的整体安全水平。而在总结过去经验的基础上，水利部门不断提炼网络安全防护的成功做法，形成了一系列可复制、可推广的防治措施。这些措施既包括技术层面的创新，如加强网络安全设备的更新升级、优化网络安全策略等，也包括管理层面的改进，如完善网络安全管理制度、加强网络安全教育培训等。通过实施这些防治措施，水利部门能够更有效地预防和应对网络安全事件，确保水利网络的稳定运行。此外，水利部门还充分利用国家多个网络安全部门的技术优势，加强了对水利重点网站和事业部门的安全监测。通过提高安全检测的频率和质量，水利部门能够及时发现并处置潜在的安全风险，为水利行业的安全发展提供了有力保障。并且，水利部门还建立了风险预警机制，对可能出现的网络安全问题进行提前预警和防范，进一步提升了水利网络的安全防护能力。

2.2 发挥互联网优势进行资源整合

为实现这一目标，水利部门引入了先进的扫描和风险评估技术系统，这些系统如同网络世界的“守护者”，对网站内部的各项信息措施进行全面而细致的审查，确保每一个细节都符合安全标准。在具体操作中，水利部门首先通过内部的安全信息管理平台，对关键的服务器、数据库以及相关的硬件和软件设备进行严格的定点检测。这一步骤至关重要，它如同对系统进行一次全面的“体检”，能够及时发现并排除潜在的安全隐患。只有当这些关键组件经过检测确认安全无虞后，水利部门的各项业务才会被允许高效运行，从而确保服务的连续性和稳定性。其次，在网络安全信息定点检测的基础上，水利部门还注重信息的收集和整理工作[4]。他们通过建立完善的信息收集机制，实时捕捉网络环境中的各种安全动态，为制定应对策略提供数据支持。同时，水利部门还制定了详细的处理策略，这些策略涵盖了从预防到应对的各个环节，确保在遭遇网络攻击时能够迅速而有效地作出反应。最后，为了进一步提升网络安全管理的效率和质量，水利部门还建立了内部的联动机制，这一机制打破了部门之间的壁垒，实现了信息、资源和技术的共享与协同。通过这一机制，水利部门能够更快速地响应网络安全事件，更有效地调动各方力量进行应对。并且，这一机制还促进了人力资源的优化配置，使得网络安全技术检测工作更加高效、有序。

2.3 完善水利网络安全预警体系

在平台的建设初期，就需将信息安全与高效性作为基石，确保平台能够稳定运行并有效抵御各类网络威胁。为实现这一目标，水利部门需投入资源，采用先进的技术手段，如大数据分析、人工智能等，对平台的信息流进行实时监控与分析。同时，预警信息的可视化也是此步骤中的关键环节。通过将预警信息以直观、易懂的方式呈现，如通过图表、报告等形式，可以帮助决策者迅速把握安全态势，及时作出反应。此外，预警机制还需具备深度分析能力，能够基于内外部收集的信息，预测可能受影响的部门及潜在的财产损失，并提前规划

应对策略，以减轻风险带来的冲击。在构建预警信息平台时，水利部门还需重视与外部第三方平台及厂商的联动。通过与这些合作伙伴的高效协作，水利部门可以获取更多关于硬件运行状况、软件更新情况等方面的信息，及时发现并解决运行过程中可能存在的弊端问题。这种内外结合的预警机制，能够显著提升水利网络安全的整体防护水平。在具体实施中，水利网络预警小组需定期召开会议，对当前的网络安全形势进行分析与研判，制定针对性的预警策略。并且，小组还需加强与各部门的沟通与协作，确保预警信息能够准确、及时地传达至相关部门，并协助其制定有效的应对措施。

2.4 建立水利网络安全信息通报机制

构建科学合理的水利网络安全信息通报机制，是实现主动防御与综合防护策略的重要基石，这一机制的建立，旨在确保水利部门能够及时、准确地获取并传递网络安全信息，从而有效提升整个行业的网络安全防护能力。（1）建立职能明确的工作部门是通报机制建设的首要任务，这一部门需负责收集、整理、分析和传递网络安全信息，确保信息的准确性和时效性。同时，该部门还需与上下级机构保持高效的联动，确保信息的顺畅流通。通过明确的职能划分和高效的协作机制，我们可以确保网络安全信息得到及时有效的处理，为决策提供有力支持。（2）在通报机制的具体运行过程中，我们需要对通报内容进行合理处置。这包括明确通报的要求和具体内容，确保信息的完整性和准确性。并且，我们还应重视通报的方式，选择适合的管理平台或电子邮件等形式进行信息传递。这些方式不仅具有高效、便捷的特点，还能确保信息的保密性和安全性，通过合理的通报内容处置和选择恰当的通报方式，我们可以有效提升信息的传递效率和利用率。（3）为了确保通报机制的高效运行，我们还需要重视通报成果的利用。相关部门应定期对通报信息进行总结和分析，提炼出有价值的信息和经验教训。这些成果不仅可以为水利网络安全防护提供基础支持，还能为未来的网络安全工作提供有益参考，通过充分利用通报成果，我们可以不断优化和完善通报机制，提升其在实际工作中的应用效果。（4）为了确保通报机制的持续完善和高效运行，我们还需要建立相应的监督和考核机制。通过定期对通报机制的运行情况进行检查和评估，我们可以及时发现和解决问题，确保机制的稳定性和可靠性。

结语

综上所述，水利网络安全监测与预警体系是保障水利信息化建设顺利进行的重要基础。通过构建全面、高效的水利网络安全监测与预警体系，我们可以及时发现并应对网络安全威胁，确保水利行业的安全稳定。未来，随着信息技术的不断发展，水利网络安全监测与预警体系将不断完善和优化，为水利行业的可持续发展提供有力保障。同时，我们也应持续关注网络安全领域的新技术、新动态，不断提升自身的网络安全防护能力。

参考文献

[1]水利部印发关于推进智慧水利建设的指导意见和实施方案[J].水利建设与管理,2022,42(01):5.D

[2]全省水利信息化管理提升三年行动方案[J].山西水利,2021(12):25-29.

[3]庄磊.山东省水利系统网络安全工作探索[J].水利信息化,2021(05):79-83.

[4]黄锐,王妍,谷立成,赵满胜.刍议水利网络安全实战演练的攻与防[J].水利信息化,2020(06):27-31.