Software Engineering and Applications 软件工程与应用, 2021, 10(4), 463-466
Published Online August 2021 in Hans. http://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2021.104051

Hans汉斯

基于气象业务信息化发展的网络安全治理研究

姜　慧

菏泽市气象局，山东　菏泽
Email: 842478318@qq.com

收稿日期：2021年7月12日；录用日期：2021年7月21日；发布日期：2021年7月28日

摘　要

随着信息化高态势发展，各类网络安全事件频繁发生，网络安全愈发突出。气象业务系统作为国家级的关键信息基础设施，在网络安全问题面临着严峻的挑战。本文针对影响气象网络安全存在的问题，提出提升气象信息网络安全的治理技术，推动气象业务现代化发展。

关键词

气象业务，信息化，网络安全，治理技术

Research on Network Security Governance Based on the Development of Meteorological Service Informatization

Hui Jiang

Heze Meteorological Bureau, Heze Shandong
Email: 842478318@qq.com

Received: Jul. 12th, 2021; accepted: Jul. 21st, 2021; published: Jul. 28th, 2021

Abstract

With the rapid development of informatization, various types of network security incidents occur frequently, and network security has become more prominent. As a national key information infrastructure, the meteorological service system faces severe challenges in network security. Aiming at the problems that affect the security of meteorological network, this paper proposes governance technologies to improve the security of meteorological information network and promote the modernization of meteorological business.

文章引用: 姜慧. 基于气象业务信息化发展的网络安全治理研究[J]. 软件工程与应用, 2021, 10(4): 463-466.
DOI: 10.12677/sea.2021.104051

Keywords

Meteorological Business, Informatization, Network Security, Governance Technology

1. 引言

气象业务信息化系统是国家级的关键信息基础设施，对各项生产经营活动有着重大的意义。随着各类信息技术的不断涌现和发展，在推动气象网络现代化发展的同时，气象发展的外部环境逐渐趋于复杂化，各类网络安全问题频繁发生。网络是气象数据传输和共享的基础平台，只有保证气象网络的安全，才能有效提升气象业务工作效率。各级气象部门信息系统网络主要包括气象业务内网、局域网、实现国、省、市、县四个节点互联互通的气象业务专网、依托政务外网的国家突发事件预警信息发布系统[1]。随着气象业务信息化快速发展，虽然气象信息系统安全建设取得了一定的成绩，但随着气象云和气象大数据建设的不断推进，网络安全形式愈发严峻，气象业务信息系统安全仍然面临着严峻的挑战，因此，发展网络安全治理技术尤为重要。

2. 气象业务信息化发展中的网络安全问题

结合国内外气象部门的相关数据分析，随着信息化的高速发展，对气象网络平台造成安全隐患的情况主要是病毒威胁、非法访问、平台信息非法盗取、黑客攻击等危害，严重影响气象信息网络系统安全和气象业务平台的正常运行，导致各类网络安全事件产生的问题主要包括以下几个方面。

2.1. 网络病毒和非法入侵

气象网络信息安全平台最大的威胁是病毒入侵，随着各类新型信息技术不断发展的同时，各种新型病毒的种类在不断更新，且更新的速度快，传播的频率高。基于气象网络信息平台发展尚不完善的特点，网络病毒会根据气象网络信息平台系统所存在的漏洞着手，趁着系统更新、装配等时机，采用多种手段对平台开展侵入和和危害，导致平台被病毒感染，影响气象业务的正常运行，严重的甚至导致网络全面崩溃，给气象部门带来巨大的损失[2]。因此，气象部门人员应提高防范病毒的意识，确保网络信息安全工作顺利实施。

互联网是独立于虚拟世界并具备高度开放性的空间，该空间没有准入门槛，人们可以自由地利用虚拟身份信息获取信息、相互交流，很多系统具有漏洞的信息平台遭到黑客的入侵和攻击，难以实现对气象网络信息安全的有效保护[3]。

2.2. 安全监管不足

信息安全管理工作缺乏有效的监督，对网络安全的重视程度不够，安全培训不到位，缺乏计算机信息系统安全的安全防范和意识。其次，气象网络信息平台和系统普遍存在专业度比较低的现象，很多基层气象单位没有专业的气象网络技术开发和管理人员，信息网络平台存在一定的安全隐患，隐患一旦爆发，将会对业务系统带来一定的影响[4]。气象业务管理人员在日常工作中没有及时对系统和软件进行更新，容易受到病毒或恶意软件的攻击。另外，网络安全设备老旧，没有充足资金的投入采购设备，无法

有效阻止新的恶性软件和病毒的入侵。

3. 提升气象信息网络安全的治理技术

3.1. 强化落实信息网络安全责任制

高度重视信息网络安全保护工作，严格依据国家法律法规以及地方、上级主管部门的要求，充分认识网络安全的重要性和紧迫性。按照“谁主管谁负责，谁运营谁负责”的原则，主要领导要考前指挥，层层落实网络安全责任，确保网络安全工作分工明确，责任到人，全面落实信息网络安全管理责任制，建立考核和网络安全责任追究制度，确保信息网络安全工作落实到位。

3.2. 强化信息网络安全管理制度建设

修订和规范各种安全管理制度，包括计算机安全管理制度、机房安全管理制度、网络安全管理制度、网络信息安全突发事件应急预案、气象业务专网安全管理制度、信息系统运行维护管理制度、信息系统信息发布制度、信息系统建设管理制度、计算机及网络安全保密工作实施方案、终端与介质安全管理、人员安全管理制度、网络安全宣传、教育和培训等。

3.3. 强化信息网络防护技术

1) 加强物理层面防护

物理安全策略是指计算机在安全的物理环境下，保障计算机网络安全。物理安全主要是保障线路通断和软、硬件的安全可靠。加强应急基础保障，主要是通信电缆、UPS 电源、机房场地环境等基础设施，机房要具有一定的防水防火和抗干扰的能力，UPS 电源和发电机等设施要保障到位，确保在突发情况下完成电力供应。

2) 加强网络安全建设

对部门内的系统梳理和筛查，确认测试系统、老旧系统等情况，对无人负责、无任何安全防护措施的网站、测试系统、老旧系统等及时关停。排查出潜在风险隐患，确保出现网络安全事故时，能在规定的时间内有效地处理，将网络安全事故的带来的影响和损失降低到最低。

3) 加强网络安全设备规划部署

无线网络仅限于连接互联网。对无线设备和网络实行统一管理，对接入无线的终端进行实名认证、网络准入和上网管控，且在重大社会活动举行期间要停用无线网络。采用网闸[5]的部署方式实现系统内网和外网的隔离，网闸能阻断具有潜在攻击可能的一切连接，使黑客无法攻击、无法入侵、无法破坏，实现真正的物理隔离。在网络边界部署下一代防火墙[6]，通过下一代防火墙的防病毒网关模块，实现对恶意代码的检测和清除。通过入侵检测系统(IPS)，针对用户行为分析检测，对网络进行监测，提供对内部攻击、外部攻击和误操作时的实时保护。通过上网行为管理，能够进行安全审计，对部门内员工的上网行为进行控制。通过部署网络安全分析与管理设备，针对信息系统平台遇到的威胁情报告警信息、网络攻击等安全问题进行针对处理。

4) 加强网络管控

网络安全设备管理要求对登录网络设备的用户进行身份鉴别，对网络设备的管理员登录地址进行限制，设置的口令应符合要求且定期更换。每个终端计算机和服务器都要安装杀毒软件，并及时更新病毒库，实时监测修补系统漏洞，针对性调整防护，强化管理措施、提高风险控制、漏洞加固等工作，加强在防篡改、防病毒、防攻击、防瘫痪、防泄密等方面的有效性。涉密计算机要设置复杂口令，由业务管理人员保管负责，关闭或删除不必要的应用、服务、端口和链接，加强 VPN 系统和移动应用对用户的身

份识别和权限控制。

5) 强化信息网络安全应急演练和应急处置能力

信息网络安全应急演练是健全信息网络安全运行机制，检验信息网络安全应急预案和业务技术专项应急预案的有效性，是相关组织和人员对网络安全突发事件的应急处置能力的体现，保证各项应急调度指挥工作高效、有序地进行。通过网络安全演练，进一步完善、熟悉网络安全应急预案，充分做好应急响应准备，确保能够及时发现、报告和处置网络安全突发事件，不断提高应急处置能力。

6) 做好信息安全等级保护

《网络安全法》于 2017 年 6 月 1 日起正式实施，它是我国第一部有关网络安全的国家法律，在气象网络安全治理方面具有重要的指定意义，网络安全法规定各运营使用单位要开展网络安全等级保护制度。以网络安全和信息安全等级保护 2.0 [7]指导，根据《网络安全等级保护基本要求》[8] [9]，以保障气象业务系统的安全运行为目标，各运营使用单位按照要求选择具有资质的评测机构，对信息系统安全保护状态开展等级测评工作。加强信息系统建设，提升气象业务信息的基线安全能力。

4. 结语

网络安全已经成为事关经济发展、国家长治久安和人民群众福祉的重大战略问题[10]。信息化技术的不断发展在给我们带来便利的同时，意味着气象信息化发展将会面临更为复杂的发展环境，这就对气象部门的网络安全方面的治理技术提出了更高的要求，需要气象部门不断提高防范和抵御风险的能力，增加相应的安全防护措施、加强信息网络安全管理工作、提升安全防护技术手段，从而提高气象信息的整体安全，为气象事业现代化发展提供坚实的网络基础。

参考文献

[1] 谢国权, 郑伟才, 张锋, 等. 基于国家突发事件预警信息发布系统的数据对接与应用开发[J]. 气象科技, 2018, 46(6): 1130-1135.

[2] 刘东君, 何恒宏, 谭振, 等. 气象网络安全治理体系研究[J]. 网络安全技术与应用, 2019(2): 90-92.

[3] 田征, 李楠, 弋小虎. 浅析网络安全态势感知技术在气象网络中的实践与应用[J]. 网络安全技术与应用, 2020(5): 139-140.

[4] 马强. 市级气象部门的气象信息网络安全问题及其对策[J]. 南方农业, 2018, 12(9): 137, 140.

[5] 江彩英, 郭晓佳, 谢丹, 林凯特. 深化市, 县级气象信息网络安全治理研究[J]. 2019(12): 131-134.

[6] 王扣武, 张珺铭, 王婧如. 基于下一代防火墙的企业网络安全设计与实现[J]. 信息技术与信息化, 2019(6): 123-126.

[7] 曲洁, 范昡玲, 陈广勇, 等. 新时代下网络安全服务能力体系廸设思路[J]. 信息网络安全, 2019, 19(1): 83-87.

[8] 黎水林, 陈广勇, 陶源. 网络安全等级保护测评中网络和通信安全测评研究[J]. 信息网络安全, 2018, 18(9): 80-85.

[9] 马力, 祝国邱, 陆磊.《网络安全等级保护基本要求》(GB/T 22239-2019)标准解读[J]. 信息网络安全, 2019, 19(2): 77-84.

[10] 马卓元, 杨向东, 闫育芸, 等. 基于信息系统安全测试人员能力认证的设计[J]. 网络安全技术与应用, 2019(8): 7-8.