浅谈民航空管气象网络安全隐患及应对策略

诸淑香
民航贵州空管分局

[摘　要]本文重点分析了民航空管气象网络中存在的安全隐患，基于民用航空网络安全等级保护基本要求，提出了空管气象网络安全应对策略。

[关键词]空管气象网络；安全隐患；应对策略
【DOI】10.12252/j.issn.2096-627X.2021.10.1146

一、引言

近年来，全球网络安全局势已然变得更加复杂。随着5G、大数据、云计算、AI、物联网等新技术的融合发展，网络威胁持续进化升级，从普通网络犯罪上升到有组织地与国家对抗，攻击目标从针对普通民用设施到瞄准关键信息基础设施，变得更加棘手、难以应对。同时网络攻击手段不断升级，呈现多样化趋势，勒索蠕虫、高级威胁APT、数据泄露、供应链攻击等安全事件频频发生，网络威胁呈逐年上升趋势，民众生活、经济生产、社会稳定、国家安全遭遇巨大风险。

民航气象信息网络，承载着大量重要的各类实时气象资料和航空气象产品，机场气象台需要将这些资料准确、及时地提供给航空用户，并按照规定与上级单位进行飞行气象情报交换。最大限度地为飞行安全、稳定、高效提供强有力的保障，是民航运输体系中的重要组成部分，是国家网络安全的重中之重。因此及时梳理民航气象信息网络存在的安全漏洞，对症下药，提出切实有效的防护措施，构建一套完备的网络安全防护体系势在必行。

二、空管气象网络安全隐患分析

（一）自然因素

空管气象网络涉及的设备多而复杂，业务分布广泛，设备检修难度较大，暴露在室外的探测设备和通信线缆容易受到雷电、电磁干扰、虫鼠啃咬、建设损伤风吹日晒损耗等的破坏，直接影响到数据传输质量，轻则造成通信节点、通信线缆故障，导致各类气象实时数据和服务提供延时或中断，影响气象业务可用性，重则造成关键大型设备损毁，网络整体瘫痪，造成不可估量的损失。

（二）人为因素

人为原因主要分为内部和外部两方面。内部：1.因维护人员的操作不规范、操作失误，极有可能影响到数据传输的实效性和准确性，重要气象技术装备的正常运行；2.网络安全意识淡薄，例如登录用户名密码设置过于简单且未按要求定期更换，杀毒软件病毒库更新不及时，远程管理未使用加密协议方式，将移动存储介质在生产网和外网交叉混用，增加了非法入侵的概率。外部：人为的恶意攻击行为，例如黑客入侵、发布并传播网络病毒，以此对气象情报进行窃取、暴露甚至篡改。

（三）网络缺陷

空管设备更新换代较慢，老旧的计算机系统在软件和硬件上存在一些安全漏洞，增加了木马程序、黑客入侵的可能性，使得计算机系统安全性大幅度降低。目前笔者所在单位大部分服务器采用Linux系统,用户终端采用Windows系统,而因Windows系统市场占有率高，不开源导致安全漏洞较多，更容易遭受黑客攻击，例如最近几年比较著名的“勒索病毒”，利用Windows系统的漏洞，对目标主机进行入侵，破坏用户数据，对用户造成了重大损失。另外一些应用软件本身存在设计缺陷，加之未进行定期的软件升级和漏洞修复，也容易给不法分子的破坏及入侵提供可趁之机。

空管气象网络采用二层架构形式，各业务系统通过VLAN进行划分，各用户终端通过接入层交换机连接到核心交换机，通过核心交换机上部署的VLAN网关进行数据交、转发，区域边界部署防火墙进行内外网隔离，基本能满足当下业务运行需求，但也存在一些缺陷。1.未根据承载业务类型和重要性划分不同的网络区域，未对核心业务区域进行重点保护，未对用户进行分级，实现访问控制最小化；2.核心层网络采用冷备方式工作，未实现热冗余备份，一旦主用网络设备故障，很容易导致气象业务交换网瘫痪，从而造成飞行气象情报及气象资料中断提供的严重后果；3.区域边界虽然部署了防火墙，但是一部分防火墙采用透明模式工作，未配置访问控制策略，另一部分则未严格按照业务需求配置最小访问控制权限的安全防护策略；4.不能保证通信过程中气象数据的完整性和保密性。

三、空管气象网络安全隐患的应对策略

（一）加固物理环境防护

物理环境安全是网络信息系统安全的前提，主要包括场地、设备、介质三个方面。1.场地安全是指系统所在环境的安全，本文中主要描述场地与机房。为了有效合理地对场地进行保护，机房应设置在具有防风、防雨、防震等能力的建筑内，并做好防水防潮、防火、防静电等防护措施；应配备恒温恒湿精密专用空调设备，对机房的温湿度进行调节，保证设备在适宜环境中平稳运行；应配备UPS和燃油发电机等备用电力供应设施，对UPS、燃油发电机进行定期维护、充放电测试，保证蓄电池的活性，防止因突然断电导致系统运行异常；同时机房出入口应配备电子门禁系统，严格控制、鉴别和记录进出的人员。2.设备安全主要包括设备的防盗与防毁、防电磁信息泄露、抗电磁干扰及电源保护等内容，应对设备或主要机柜进行固定，并设置明显标识，将通信线缆铺设在隐蔽安全处，设置机房防盗报警系统或有专人值守的视频监控系统，对关键设备实施电磁屏蔽，做好电磁防护措施。3.介质安全是指介质本身和介质数据的安全，应将介质存放于安全可靠、温湿度适宜的环境内保存，避免因介质的物理损伤导致数据丢失，同时做好安全删除和安全销毁工作，避免删除不当导致敏感数据被他人窃取。

（二）构建“一个中心”下“三重防护”的安全体系

1.安全管理中心：规划特定的安全管理区域，在此区域部署堡垒机和审计管理系统，其中堡垒机可实现角色账户三权分立，对登录用户进行统一身份验证，对运维行为进行安全监控，接管运维终端对目标资源的直接访问。通过部署审计管理系统，建立统一的安全审计管理平台，可实现统一收集各业务系统的审计数据，提供审计数据的查询、溯源、统计服务。以此建立一个“安全管理中心”，实现对网络中所有的主机、通信线路、网络设备、安全设备等的运行情况进行统一集中监测和管理，对网络异常事件进行识别、报警和分析。

2.安全通信网络：优化网络架构，提高网络的数据传输效率、可靠性、安全性。首先应根据承载业务类型和重要性，将生产网划分为民航数据库系统、气象台局域网、资料交换区、核心交换区、安全管理区等网络区域，并为各网络区域规划IP地址，在区域与区域之间部署防火墙，实现区域间的有效隔离。其次应考虑环网传输链路、无线传输链路、民航TDM网双路热备份传输、核心层网络双机热备等建设方案，保证关键网络节点、关键传输链路的硬件冗余，通过以上措施保障空管气象业务平稳高效运行。

3.安全区域边界：充分利用防火墙技术，建立牢固的区域边界。防火墙是隔离在可信网络与不可信网络之间的一道防御系统，一般安装在内部网与外部网交界处，可以根据预定的安全规则监视和控制传入和传出的网络流量，具有很好的网络安全保护作用。因此，在空管气象网络边界处，应部署防火墙、隔离网

闸等安全设备，做好防火墙安全策略配置，进行强逻辑隔离和访问控制。边界防火墙的配置主要有四个方面：1.对生产网进行安全区域划分，实现对内部网络关键业务的隔离保护；2.根据空管气象业务实际需求设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信，建立基于白名单的访问控制机制；3.应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；4.配置精细IP访问策略、IP准入防护策略，通过对源地址、目的地址、源端口、目的端口和协议等进行检查，实现对出入网络的信息流进行有效控制，过滤掉不安全服务和非法用户。

4.安全计算环境：即主机安全，主要包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范等内容。网络中的服务器、终端应完善安全基线设置，加强密码复杂度，禁止弱口令，利用堡垒机实现定期改密、远程加密管理网络设备；授予用户所需的最小权限，关闭删除过期或多余的账户；应关闭不需要的系统服务、默认共享和高危端口，定期进行漏洞扫描、风险评估和补丁升级，防范恶意软件攻击。

（三）制定严格的网络安全管理制度,增强维护人员的网络安全防范意识

建立一套规范化的网络安全管理制度，提高维护人员的网络安全防范意识与网络安全事件应急处置能力，对于加固空管气象网络安全屏障意义重大。首先应针对安全管理活动的主要管理内容一一完善安全管理制度，完善各生产设备的操作规程，建立一个科学的防病毒系统，购置正版杀毒软件，定期巡检内部网络的安全性、各系统的漏洞情况、杀毒软件及病毒库版本号，及时更新病毒和补丁库，增强网络系统免疫力。其次应定期组织相关人员进行安全意识教育和岗位技能培训，实行定期技能考核制度，以此增强工作人员的安全责任意识，提升网络安全知识储备。

四、结语

当下，面对网络安全的复杂形势和艰巨任务，民航空管气象部门必须提高网络安全防护意识，改变惯有的维护维修手段，提升网络安全维护技能，持续加强在网络空间安全的投入力度，完善网络空间布局，持续提升网络攻防能力。强化政策标准引导，根据《网络安全法》等相关法律法规，因地制宜地完善本单位网络安全管理制度，运用标准引领和规范网络安全工作。从“人机料法环”五个环节着手，加强空管气象网络安全监督检查，推动安全问题整改，全面提升空管气象整体网络安全水平。

参考文献：

[1]MH_T 0076-2020 民用航空网络安全等级保护基本要求

[2]吕运洲,闫春旺,王彦朝.浅谈气象网络安全隐患的排查方法与应对策略[J].中小企业管理与科技(上旬刊),2020(11):62-63.

[3]邓力涌,梁苑苑,张小琼.基于等保2.0的广西气象网络安全防护策略[J].气象研究与应用,2021,42(03):99-103.

[4]马杰,王景海,李芙蓉. 基于等保2.0的网络安全防护体系设计与实施[C]//.中国新闻技术工作者联合会2020年学术年会论文集.[出版者不详],2020:143-149.

（上接第1911页）

有许多控制专用硬件，以实现切断网络间连接的链路层连接，并且能够为网络中的数据交换提供安全的网络环境。一般网闸的硬件部分分为三个组成部分，即内部处理单元、外部处理单元以及隔离安全数据交换单元。尽管网闸能够实现内外网之间的隔离，但是依然可以保证数据以“摆渡”的方式在两个网络间进行信息的传输功能。网闸能够有效阻隔外部的安全威胁，阻止较多木马病毒的入侵，保证内部网络的安全性与数据不被删除、篡改，维护气象信息网络数据安全。

3. IPS入侵防御系统对外网数据进行过滤。

IPS是入侵预防系统的缩写，是在外部网络防火墙中架设的一台网络安全设施，是对防火墙和防病毒软件的补充设施。该系统能够对网络设备或网络中传输的数据资料进行监视，当发现传输的数据中含有伤害性数据时可以及时对数据进行调整、隔离等操作。在气象信息网络中添加IPS能够及时识别出对网络有攻击性的程序和代码，及早帮助技术人员发现安全风险，阻止外部非法人员对网络的入侵。甚至在必要时还可以为民航部门提供入侵者的入侵证据，方便追究法律责任。

4.采用MSTP+OSPF+VRRP的冗余网络架构。

MSTP+OSPF+VRRP的冗余网络架构具有安全性高、稳定性好的优势，保证数据传输顺利。MSTP可以有效解决气象信息网络中设备环路的问题，备份接入交换机的双上行链路，分担业务流的负载。OSPF的动态路由能够对核心交换机和ATM路由器间的路由设备进行学习，最终得到多条路径以保障出口链路的负载稳定和负载均衡。VRRP是把两台不同的核心交换机中的地址进行虚拟处理，得到的虚拟IP对用户提供相应的网关服务，这样可以保证一台核心交换机发生设备故障，网络能够在第一时间切至另一台交换机中。采用MSTP+OSPF+VRRP的冗余网络架构可以在数据交换节点一旦出现问题时，及时改变数据线路，保障数据的稳定传输。

5.优化信息安全防护系统。

要想保障气象信息网络的安全，还要在外部服务器与内部局域网里继续优化防护系统，实现24小时的全天候实时监控网络。结合云端服务器与大数据分析，不断更新升级防护技术与病毒库，还可以引入B/S的可移动管理系统，能够方便管理人员随时随地的登录控制系统，对气象信息网络的安全进行实时防护与监测

（二）增加设备的自身可靠性

除了上述的技术手段外，还可以对设备升级以提升其性能的可靠性。包括使用双机结构的服务器、设置能够独立存放数据信息的磁盘阵列系统，提升无线设备连接网络的安全性等。从多个方面入手提升系统的信息安全性能。

四、结语

由于网络信息技术的发展极为迅速，黑客使用的攻击手段也越来越高明，气象信息网络作为保障民航飞行安全的重要安全环节，提升气象信息网络的安全性是所用专业技术人员亟待解决的难题。目前对于该问题已经通过多种手段对网络的安全进行了防护，但是我们不能就此安于现状，要想做好网络信息安全防护，还需要技术人员技术钻研探究，为人民的生命财产安全和民航的正常运行提供技术保障。继续加深各个学科间的技术交流与融合，采用多种安全防护手段来提升气象信息网络的安全性，是网络安全管理发展的必然趋势，需要全体技术人员的继续努力探索。

参考文献：

[1]张斌.天津空管气象信息网络安全保护建设新进展[C]//第33届中国气象学会年会 S20 气象信息化——业务实践与技术应用.中国气象学会, 2016.

[2]袁野.西南空管气象信息综合服务系统的研究与设计[D].电子科技大学, 2011.

[3]张斌.民航空管气象网络安全建设方案设计与实现[J].计算技术与自动化, 2014（1）.

[4]高永强,郭世泽.网络安全技术与应用大典[M].人民邮电出版社, 2003.

[5]赵立成.气象信息系统[M].气象出版社, 2011.

[6]格贝奈,孙贤和.面向服务的通信体系结构:英文[M]. 清华大学出版社, 2007.