民航空管气象网络安全建设方案设计与实现

殷昕旺
民航贵州空管分局

[摘　要]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。目前对于气象信息的网络安全体系包含“网络管理软件、硬件防火墙与防病毒软件”，为了适应网络技术的发展，维护气象信息安全，还需要进一步完善网络服务器、提高设备的故障检测技术以及互联网入侵监测系统等，最终以实现气象信息安全的全方面、多层次的网络防护体系。本文以民航气象信息网络安全管理体系中应用的防护技术为起点，介绍了目前较为常用的技术设备，希望能够为其他从业者提供一些技术参考。

[关键词]民航；空管；气象网络安全；网闸
【DOI】10.12252/j.issn.2096-627X.2021.10.1145

一、引言

随着我国互联网的快速发展，气象信息的网络安全也同样备受关注，针对气象信息安全发展的相应网络安全技术也迎来了新的机遇和挑战。目前对于气象信息的网络安全体系包含“网络管理软件、硬件防火墙与防病毒软件”，但是为了适应网络技术的发展，维护气象信息安全，还需要进一步做到完善网络服务器、提高设备的故障检测技术以及互联网入侵监测系统等，最终以实现气象信息安全的全方面、多层次的网络防护体系。

目前我国民航部门的空管信息系统具有涉及应用多、规模大和业务依赖性强的特点，因此一旦受到攻击，会对民航的正常运行造成不可估量的损失，也是对民航安全的极大威胁。空管信息系统的网络安全建设，能够有效保护信息安全不被侵犯，减少信息资源所面临的风险，在最大程度上收获最大利益。另外，完善空管信息的安全还可以对空管信息服务水平、保障设施与基础设备的可控性、保密性、可用性与完整性不受影响，这是保障我国社会稳定、经济发展与国家安全的必要保证。建立科学有效的空管信息网络安全保障系统是目前我国民航发展的必行之策。

正是由于计算机与互联网技术的飞速发展，使得气象网络的地位逐步提升，所需要承担的信息交换和数据传输的工作量愈发增长，维护气象网络安全有了更迫切的要求，需要广大从业者不断提升个人技术，在防御病毒、监测入侵与网络结构改革等多方面完善气象信息安全网络防护系统，为我国的信息安全添砖加瓦。

二、民航气象网络信息安全现状

（一）气象网络的信息安全现状

目前我国正处于网络技术飞速发展的腾飞阶段，不论人民的日常生活还是生产工作都离不开网络支持。电子商务与政府机关对于互联网应用有很大的需求，随之而来的就是维护网络安全的重要意义。自中国与国际社会的互联网连接后，我国已经受到了多次来自国外黑客的网络攻击，并且网络攻击无时无刻都在发生，这对我国的网络安全造成了威胁。保障我国的网络环境安全，就是保障我国的政治安全、文化安全、经济安全、军事安全、国防安全，避免我国陷入经济战与信息战的不利境地。

对于我国民航系统中的气象信息网络来说，其内部存有大量的重要航空实时数据与航空气象信息的绝密资料，所以保证其网络安全具有非常重要的意义。若民航部门的气象信息网络受到攻击造成资料泄露或失去控制，会为航空公司的机组成员与地面塔台中的管制员带来极为严重的威胁，尤其是重要的天气资料，如果丢失或被篡改了数据，甚至会导致航空事故的发生，危害到人民群众的生命安全，为国家带来无法估量的损失。

近些年来，民航对于气象网络的信息化建设越来越重视，在很大程度上促进了气象网络的信息化发展，随之而来的便是VPN远程访问的频率增长。气象网络一般分为内网与外网两部分，前者包括气象观测与预报、数据库、通讯设备、卫星云图、雷达等众多终端设备，外部网络连接着各大航空公司用户。内、外网络之间是相对独立又互相连接的，二者需要不断进行信息交互以完成气象网络的日常工作，但是恰恰是外网与航空气象内部网络的连接，造成内网的安全隐患与威胁，黑客可以由此入手发动攻击，窃取气象信息或导致气象网络瘫痪。特别是无线通讯技术的发展使得外部用户可以摆脱有线终端的地理限制，随时随地就可依靠移动终端进行信息查询，一方面提升了用户的网络使用体验，方便用户查询实时气象数据，另一方面也使得内部网络的信息安全性受到了更多被攻击的可能。那么，如何既能保证内部网络的信息安全，又可以确保外部网络用户使用顺畅，是民航气象网络信息网络建设工作中必须要解决的问题。

（二）现行网络安全常用措施

在这样严峻的网络环境中，当前我国常用的安全防护方法以设立防火墙为主。通常的做法是在内部与外部网络之间使用防火墙进行隔离，以及在内网与专网之间采取物理隔离的方法来维护气象网络的信息安全。具体来说，逻辑隔离一般依靠安装的PIX515E防火墙来确保内外网之间的安全，物理隔离则需要网闸等设备。

同时，为了向广大用户提供实时气象的信息查询功能够顺利应用，会使用支持跨平台且具有B/S架构服务的模式，利用无线远程传输的方式把气象网络中的实时信息传给每一位用户的智能手机、笔记本电脑以及平板电脑等无线移动设备。但是为了能够确保传递信息准确且不被篡改，还需要采取更加安全有效的内、外部网络连接的方式。所以我国常用网闸与防火墙、VPN认证和IPS以及网络结构优化等多种加固信息安全的措施，综合应用以保障数据能够安全地传送到用户手中。

三、民航气象网络信息安全建设策略

（一）改进气象网络总体架构

1.扩展服务器外接的范围。

为了满足日益增长的用户数量与查询需求，气象信息网络可以增加对外接口的数量与带宽，特别是不同用户选择的线路不同，所以最好能够将现有使用最广泛的两个网络——联通和电信接入气象信息网，满足不同用户的使用。这样将外接口由单一线路改成双线路与外部网络对接之后，用户就可以依据自己的网络线路选择对应的线路进行访问，并且要在两条线路中都安装能够访问到控制列表的内、外部网络防火墙，以防某一线路故障后，不会影响用户的正常使用，用户只要更换下地址就能使用另一正常线路来访问浏览器。

另外，为了确保气象信息不被泄露，用户必须在安装了VPN认证软件之后才可以登录气象信息网络，这样能够阻止非法用户窃取机密信息，保护气象信息网络安全。并且通过防火墙进行的远程用户在访问的时候需要先经过IPS入侵防御系统的安全过滤再通过交换机转移至服务器内，提高气象信息网络内部的安全性。

2.网闸对内部与外部网络的隔离。

考虑到气象信息网络系统中内外部网络间的信息交换是单向的，也就是将内部网络中的数据资料提供给外部网络中的用户终端，所以最合适的物理隔离方式便是使用网闸来实现内、外部网络间的安全保护。

网闸是安全隔离网闸的简称，其概念是指一种电路中包含

（下转第1913页）

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.