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(3):99-103.
Deng Liyong,Liang Yuanyuan,Zhang Xiaoqiong.Guangxi meteorological network security protection strategy based on Network Security Level Protection 2.0 Standard[J].Journal of Meteorological Research and Application,2021,42(3):99-103.

基于等保 2.0 的广西气象网络安全防护策略

邓力涌，梁苑苑，张小琼
（广西壮族自治区气象信息中心，南宁 530022）

摘要：结合广西气象部门的信息网络安全现状，提出了基于网络安全等级保护 2.0 标准的广西气象信息网络安全防护策略,通过对策略的具体实施和应用,气象网络各安全域边界的主动防御能力、安全管理区的态势感知及溯源能力、大数据云平台终端安全防护能力等各方面能力得到了提升,提高了气象信息网络安全防护能力。

关键词：信息网络安全;等级保护 2.0;安全防护策略;气象网络
中图分类号：P409 **文献标识码**：A **doi**：10.19849/j.cnki.CN45-1356/P.2021.3.17 **OSID**：

引言

网络安全等级保护制度 2.0 标准（以下简称等保 2.0 标准）作为我国网络安全领域的一项基本制度,对加强我国网络安全保障工作,提升网络安全保护能力具有关键指导作用。等保 2.0 标准提出“一个中心三重防护”的安全防护框架,气象部门建立以计算环境安全为基础,以区域边界安全、通信网络安全为保障，以安全管理中心为核心的气象网络安全体系,是广西气象网络安全研究的重点。

按照中国气象局信息化发展方向，在网络安全等级保护 2.0 新标准体系下，不断完善广西气象网络安全基础建设[1],深入剖析广西气象信息网络安全面临的问题,加强顶层设计,制定基于网络安全等级保护 2.0 标准的广西气象信息网络安全防护策略,进一步完善广西气象网络安全基础架构,对气象业务系统的安全可靠运行具有重要意义。

1 广西气象网络安全现状分析

广西气象部门网络安全防护能力逐年提升,在各个边界部署了防火墙，在安全管理中心也部署了态势感知系统、行为审计、扫描系统等设备,同时配置了安全防护策略。但是,近几年随着严峻的内外部网络安全形势变化和新技术的不断发展，现有网络安全防护策略已经无法满足广西气象事业发展对网络安全的需求，虽然全区各单位也部署了一些网络安全产品和开展了系统等保测评，但没有明确统一的标准和要求。自治区气象局直属单位、市气象局和县气象局都有互联网出口，而网络安全威胁主要来自互联网攻击，过多的互联网出口遭受到的网络安全攻击防不胜防[2],往往一点突破全网遭殃。目前广西气象网络安全现状主要体现以下几点：

（1）物理环境安全。广西气象局的大数据中心机房按照 A 级机房标准建设,基本满足等保 2.0 标准,但是在外部人员进入机房的审批制度还不够完善，在电子门禁系统和监控系统的配套未能与时俱进。

（2）通信网络安全。广西气象通信网络架构属于省-市-县三级架构,在省、市两级均划分有不同的网络区域,基本满足三级等保的网络安全基础架构,但是在可信验证方面,除自治区气象信息中心负责的虚拟专用网(VPN)系统外,存在个别单位自

收稿日期：2021-04-16
基金项目：国家网络安全等级保护制度新标准背景下广西气象信息网络安全联防体系及安全策略研究([2020]第 201 号)
作者简介：邓力涌(1988—),男,硕士研究生,工程师,从事气象信息网络工作。E-mail:1042613768@qq.com

建VPN 系统的情况,并且 VPN 没有配备双因子认证策略。

(3) 区域边界安全。广西气象部门网络边界主要包括:气象外网边界和气象内网边界,在边界部署有边界防火墙,但是边界防火墙的安全防护策略没有按最小访问控制权限的要求配置,并且也没有按等保 2.0 标准部署流量清洗、入侵防御、web 防护、网页防篡改等网络安全设备。

(4) 计算环境安全。除自治区级各直属单位办公终端开展了入网准入控制外,广西其他单位的终端和主机普遍没有入网准入控制措施,入网终端的 IP 地址暂未与 MAC 地址进行绑定。广西终端安全防护软件授权未能实现全覆盖,未安装安全防护软件的终端依然能访问区级核心业务系统,存在安全风险。

(5) 管理中心安全。在安全管理中心,部署有态势感知系统、终端安全防护系统、漏洞扫描系统,但是缺少安全威胁的监测、密码安全管理系统、日志分析管理系统、统一认证管理系统、安全审计系统等相关网络安全设备。

(6) 云计算安全。广西气象部门部署有气象私有云,在云平台安全部署有虚拟化终端安全防护软件,但是终端安全防护软件并没有实现全覆盖,在云主机、云数据库、云存储、负载均衡、虚拟网络等核心组件,没有按照等保 2.0 标准的要求,进行最小访问控制策略的配置,没有细化相关的访问权限。

基于等保 2.0 标准的要求,广西气象局通过建设安全管理中心支持下的三重防护结构框架部署相关网络安全设备,在安全检测、通报预警、事件调查、风险评估、应急处理、数据防护、容灾备份等方面的能力需要一进步加强,市、县气象局在互联网、气象地面宽带网、4G 备份网边界的防护能力严重不足[3],因此需要制定更完善、更精细的网络安全防护策略。

2 广西气象网络安全防护策略

2.1 物理环境防护

按照网络安全等级保护 2.0 标准,机房场地应选择在具有防震、防风和防雨等能力的建筑内;机房场地不宜选择建设在建筑物的地下室、顶层,否则应加强防水、防潮措施。机房场地应达到所承载最高级别等级保护对象的网络安全要求,其 UPS、燃油发电机等系统在需要时应能正常工作。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[4]。

建立外部人员进入机房审批相关制度。机房应配置电子门禁系统和监控系统,控制非机房管理人员进入,记录访问机房行为。机房出入口应安排专人值守或配置电子门禁系统,控制、鉴别和记录进入的人员。

2.2 气象外网边界防护

(1) 在气象外网边界(互联网、电子政务外网、行业部门专网)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。在互联网出口边界防火墙强制关闭 TCP135、137、139、445、3389、23、22 和 UDP137、138 等端口,关闭气象外网远程气象内网运维的第三方远程应用(如 TeamViewer、向日葵等)。在防火墙策略配置中,禁止气象内网地址直接映射成气象外网地址的网站、App 应用。

(2) 在气象外网边界(互联网、电子政务外网、行业部门专网)划分气象外网 DMZ 域,严格按照单向传输的数据流向标准制定安全防护策略,禁止气象外网主动访问 DMZ 区域、内网区域业务,禁止气象外网主动访问内网业务;只允许气象内网区域单向访问气象外网 DMZ 区域、气象外网区域业务,只允许气象外网 DMZ 区域单向访问气象外网区域业务。

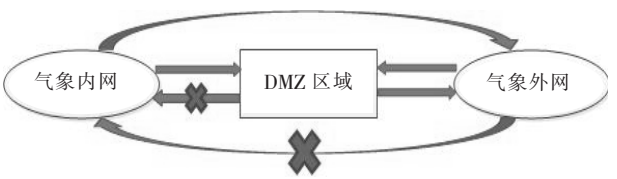

图 1 气象内网、DMZ 区域、气象外网相互访问关系图

(3) 加强流量清洗,入侵防御、web 防护、网页防篡改,根据 IP、业务系统制定流量清洗策略,实现对业务、办公人员使用带宽的限制和保障。在气象外网边界制定入侵防御策略,阻挡黑客发起的缓冲区溢出、木马、蠕虫等攻击。把对外应用的网页业务系统加入 web 防护策略,阻挡黑客发起的 SQL 注入和 XSS 等针对网站的攻击,防止网站页面内容被篡改。

2.3 气象内网防护

(1) 在气象内网数据核心边界防火墙配置精细 IP 访问策略,配置 IP 准入防护策略,IP 准入相关信息包括:终端的 IP 地址、MAC 地址,使用人和使用单位、终端名称、所属物理位置,IP 准入后才能访问

数据核心网络，在网络安全监测平台配置发现存在高危漏洞或病毒终端的策略，监测告警后人工主动断开终端网络，以防通过该漏洞或病毒攻击其他终端资源。

（2）根据安全管理需求最小化开通策略，业务系统在气象内网各网域边界配置精细访问控制策略，访问气象内网各网域的源地址必须精细到具体 IP 地址或者 MAC 地址，访问气象内网各网域的目的地址必须精细到具体 IP 地址或者 MAC 地址，访问气象内网各网域的服务端口必须精细到具体的 TCP 端口和 UDP 端口等。防火墙精细化策略示例如表1。

表 1　防火墙精细化策略示例

系统名称	源 IP（MAC）	目的 IP（MAC）	端口
广西气象业务内网	10.160.*.*	10.158.*.*	80；9000
台站 FTP 传输	10.163.*.*	172.22.*.*	20；21
财务 A++系统	10.160.*.*	10.1.*.*	443；7001
服务器远程维护	10.158.*.*	192.168.*.*	3389

（3）远程访问气象内网资源的虚拟专用网(VPN)仅供气象部门员工使用，必须且仅能由控制局域网与互联网连接的防火墙设备提供，采用双因子强认证，限制访问指定应用，对访问全程进行审计记录，对 VPN 客户端设备进行安全检测，对登录、访问行为进行异常分析与检测。要求接入网络的 VPN 客户端必须安装终端安全防护软件，用户需书面承诺对 VPN 证书及口令保密，只由个人使用，不得泄漏给他人。

（4）部署数据泄露监控功能设备，配置检查敏感数据是否有被违规发送策略，采用关键字、正则表达式、数据标识符、文件指纹、智能分类等技术集成组合策略对网络外发数据进行内容级别的检测识别，发现多种类型数据的敏感内容，对各种高风险数据外传行为执行监控或阻断的措施，保护敏感气象数据。

（5）严格禁止在局域网络内设立访问局域网络或互联网的无线网络访问设备，访问互联网的无线访问设备应与局域网络物理隔离或接入互联网对外服务区，并按国家法律法规采取网络安全管控措施[5]。

2.4 终端、服务器防护

建立广西气象部门统一的终端安全防护管理中心，入网终端有线接入实行实名登记审批，统一部署实名认证的无线 WIFI，开展全网安全准入控制，阻断不合规设备入网，保障计算环境安全。

气象内网和气象外网的网站、业务服务器（包括虚拟机）和终端电脑，必须加强密码复杂度（大小写字母+数字+特殊字符，长度不少于 8 位），禁止弱口令、默认口令、通用口令，并且关闭删除长期不用的账号，做好安全基线配置，以最小权限原则关闭主机上未使用的服务组件和端口。终端打开系统防火墙，开启访问和操作日志记录、限制登陆失败次数，关闭不使用的端口以及默认管理共享。必须安装终端防护软件，开启终端防护软件，操作系统定期升级修复补丁，修复高风险漏洞，全面查杀木马病毒[6]。

2.5 安全管理中心设计

为满足网络安全等级保护基本要求和广西气象信息网络安全的业务需求，规划部署“安全管理中心”，提出“系统管理”“审计管理”“安全管理”和“集中管控”等要求，部署态势感知系统、密码管理系统、认证管理系统、审计管理系统。

（1）部署态势感知系统，利用大数据技术，对收集的各类监测数据和内外部访问信息进行关联、分类，同时进行多维度、多模式的分析[7]，实现已知安全威胁的监测、网络安全事件过程的追溯以及未知风险的预测，结合气象业务、资产信息实现安全风险、安全事件告警的本地化服务[8]。

（2）部署密码管理系统，以国产密码技术为核心，建立完整的密钥管理体系，保障密钥全生命周期的安全，实现密码资源的统一管理，密钥在线/离线分发，密码设备的统一管理等[9]。

（3）部署认证管理系统，统一认证管理采用强身份认证的技术，以服务化方式为各信息系统提供统一的身份认证服务，实现多因素的强身份认证[10]。支持多种身份认证方式，包括静态口令、数字证书、验证短信、动态口令等，同时支持生物认证技术，具备对人脸、指纹、虹膜等生物认证技术的集成能力。

（4）部署审计管理系统，建立统一的安全审计

管理、溯源服务，提供各业务系统审计数据的查询、追溯、统计功能[11]，满足《网络安全法》和等保 2.0 标准对审计数据的存储周期(不小于 6 个月)要求。各软硬件设施将系统登录、操作、安全告警等日志记录发送至日志接收服务器，纳入统一安全审计管理。

2.6 云平台安全

气象基础云平台作为提供 IaaS、PaaS、SaaS 等云服务的云主机、云存储、云数据库等核心组件，必须及时修复漏洞，采用数据安全存储、数据加密、宕机迁移等安全技术手段[12]，保证所提供的虚拟机、操作系统、数据库、云存储等核心组件的安全性和高可用性。

气象基础云平台应当配备云安全管理平台，为气象云上各用户提供对安全资源的配置和管理，实现网络安全从创建到开通、配置、清除全生命周期的安全管理。提供面向各用户的统一身份认证、访问控制服务，提供云平台租户管理、组织管理、工作流管理、自助界面等功能，实现自动化申请安全资源、自动化审批部署。通过最小化访问控制技术，实现内部资源的访问控制权限，实时监控与审计运维人员操作，对违反网络安全的操作行为实时阻断。

3 网络安全防护成效对比分析

通过制定以上网络安全防护策略，在广西气象部门网络安全主动防御、动态防御、安全管理中心管理、可信计算、云计算防护等方面能力均有大幅提升。表 2 为根据等保 2.0 制定规则与等保 1.0 制定规则在气象部门网络安全防护能力的分析对比。

表 2 等保 2.0 防护规则与等保 1.0 防护规则防护能力对比

防护能力	等保 1.0	等保 2.0
主动防御	粗规则防护，主动防御弱	制定边界防护墙精细化规则，提升主动防御能力
动态防御	简单 IPS 防护，无动态防御能力	制定 web 防护规则、IDS、IPS 防护规则，提升网站、系统动态防御能力
安全管理中心管理	无	部署态势感知系统，制定安全感知、分析、溯源规则，提升网络安全威胁感知、溯源等管理能力
可信计算	无	制定安全准入规则，制定 VPN 双因子认证规则，提升可信计算能力
云计算防护	无	制定虚拟化、大数据云平台终端防护规则，提升云计算防护能力

4 结论

与信息等级保护制度 1.0 标准相比，网络安全等级保护 2.0 标准的严格度更高、覆盖面更广、内容更精细、角度更多元，基于网络安全等级保护 2.0 标准通过制定与实施物理环境防护、气象外网边界防护、气象内网防护、终端与服务防护、安全管理中心设计、云平台安全防护等策略，进一步提高了气象信息网络安全防护能力，广西气象各业务系统的运行得到了可靠安全保障。

构建一个能够保证网络内部用户不受攻击，数据信息不被窃取，所有业务系统、业务服务能够正常进行的安全网络架构体系，是网络安全研究的目标，在等保 2.0 标准下，通过改进网络安全等级保护 2.0 标准要求下的各项措施，进一步完善广西气象业务系统的网络安全架构，对加速提升气象现代化具有重要意义。

参考文献：

[1] 任晓炜，梁苑苑，陈婧霆，等.广西气象信息网络业务发展与展望[J].气象研究与应用，2020，41(4)：88-93.

[2] 沈晓军.广西气象局网络安全问题及其分析[J].气象研究与应用，2011，32(S2)：278-279.

[3] 邓力涌，沈晓军，陈婧霆.广西地面气象观测站备份线路的设计与实现[J].气象研究与应用，2019，40(4)：86-88，105.

[4] 国家市场监督管理总局，中国国家标准化管理委员会.信息安全技术网络安全等级保护基本要求：GB/T 22239—2019 [S].北京：中国标准出版社，2019.

[5] 戴雷雷.关于高校计算机网络信息安全及防护策略探析[J].科技创新与应用,2020(33):70-71.
[6] 杨海利.对于当前计算机网络信息安全及防护策略的思考[J].网络安全技术与应用,2020(6):2-3.
[7] 龚俭,藏小东,苏琪,等.网络安全态势感知综述[J].软件学报,2017,28(4),1010-1026.
[8] 刘冬兰,刘新,张昊,等.基于大数据的网络安全态势感知及主动防御技术研究与应用[J].计算机测量与控制,2019,27(10):229-233.
[9] 薛涛,刘潇潇,纪佳琪.大数据时代的计算机网络信息安全技术应用——评《大数据与计算机技术研究》[J].中国科技论文,2021,16(8):938.
[10] 李云飞. 网络安全等级保护 2.0 工业控制系统安全测评实践[J].网络安全技术与应用,2020(9):21-23.
[11] 王学潮.基于计算机网络技术的计算机网络信息安全及其防护方法浅谈[J].数字通信世界,2019(8):269.
[12] 贺嘉,李雁,郑袁平,等.计算机病毒防范中"云安全"的应用研究[J].网络安全技术与应用,2021(3):65-66.

Guangxi meteorological network security protection strategy based on Network Security Level Protection 2.0 Standard

Deng Liyong, Liang Yuanyuan, Zhang Xiaoqiong
(Guangxi Meteorological Information Center, Nanning Guangxi 530022)

Abstract: Combined with the current situation of information network security of Guangxi meteorological department, the security protection strategy of Guangxi meteorological information network based on network security level protection 2.0 standard was proposed. Through the specific implementation and application of the strategy, the active defense capability of each security domain boundary of the meteorological network, the situational awareness and traceability capability of the security management area, and the terminal security protection capability of the big data cloud platform have been improved, enhancing the security protection capability of the meteorological information network.

Key words: information network security; level protection 2.0; security protection strategy; meteorological network