曹波,向浩然,马园,等. 态势感知技术在省市气象部门间的联动应用[J]. 陕西气象,2025(4):74-78.
文章编号:1006-4354(2025)04-0074-05

态势感知技术在省市气象部门间网络联动中的应用

曹 波[1],向浩然[1],马 园[1],刘 畅[2]
(1. 陕西省气象信息中心,西安 710014;2. 西安市气象局,西安 710016)

摘 要:随着气象信息化的快速发展,网络攻击的复杂性和隐蔽性不断增加,新型网络攻击方式对传统安全防护提出了严峻挑战。通过对近年来陕西省气象部门网络安全防护需求的分析,设计了安全态势感知系统逻辑架构、功能,并搭建了以安全态势感知平台为中心,联动流量探针、多种防火墙的网络安全拓扑,提供了“全面监测、快速联动、一站处置”的网络安全防护工具。经 30 d 应用场景测试,系统检测出 43 台风险资产、2.01 万条有效告警,联动省市防火墙主动阻断了 362 个攻击源,在 2024 年度部门网络攻防演习中表现出良好的应用效果。

关键词:态势感知;气象信息网络;安全防护;应用场景
中图分类号:TP393.08;P409 **文献标识码**:A

近几年,陕西省气象部门的信息化水平日益提高,对外服务系统越来越多,在为各行业带来便利的同时,也使得全省气象信息网络的受攻击面不断扩大,需应对的网络攻击越来越复杂,利用未知威胁、组合攻击、高级持续性威胁[1]的新型网络攻击方式成为新的风险点[2]。传统网络安全技术往往只关注特定方面的安全状态,并不适应新型网络攻击方式[3],引入新的技术适应安全防护需求显得非常必要。

安全态势感知可以从全局视角提升对网络攻击的发现识别、理解分析、响应处置能力,集监测、预警、处置功能于一体[4]。目前已有许多关于安全态势感知技术的应用案例,杨志琼等[5]梳理了部门网络安全防护的短板,建设了珠江委网络安全态势感知平台,实现了资产管理、风险感知、预警管理等功能,提升了全局监测和主动防御能力,平稳渡过了年度网络攻防演习。呼亚杰[6]设计实现了农业农村部网络安全态势感知监测分析平台,采集各类安全设备数据进行大数据分析,以评估安全风险、自动处置安全事件。此外,黄艳红等[7]、马晋等[8]、李宏存[9]均实现了安全态势感知技术在网络安全中的应用,并取得较好的效果。因此,针对陕西省气象部门信息网络安全存在的监测不彻底、省市联动防护效果不佳等问题,引入安全态势感知技术,建立陕西省气象部门安全态势感知系统,为网络安全工作提供保障。

1 气象信息网络安全需求分析

在引入安全态势感知技术之前,陕西省气象信息网络主要采用传统防火墙对互联网边界进行被动防护,缺少主动发现、提前预警攻击的能力,在面对新型网络攻击时,往往存在监测预警能力不足、人工处置滞后、市县级防护薄弱等问题。引入安全态势感知技术是为降低这些安全风险,构建一个“全面监测、快速联动、一站处置”的安全态势感知系统,为网络安全工作提供强有力的支撑。

1.1 提升监测预警能力

新型网络攻击具有多阶段、分布式、碎片化的特征,能够绕过传统安全设备的被动防御机制,渗透目标网络[10]。这使得传统安全设备难以捕获攻击的早期迹象,导致攻击无法被及时发现,进而

收稿日期:2024-12-18
作者简介:曹波(1984—),男,汉族,陕西西安人,学士,工程师,从事信息网络与系统维护。
基金项目:秦岭和黄土高原生态环境气象重点实验室开放基金课题(2023Y-12)

使攻击者具备更长的潜伏时间,造成严重的数据泄露或业务中断等后果。因此,必须通过先进的威胁情报、多源数据融合、威胁分析等技术,早发现、早预警网络攻击,使得安全管理从被动防御转向主动防御,有效降低安全事件发生的概率。

1.2　形成一站式闭环管理

在引入安全态势感知技术之前,陕西省气象信息网络采用的安全防御手段包括:接入控制、边界防御、终端防御等。所涉及的安全产品包括:防火墙、杀毒软件、单因素 Token 等。这些单点产品独立运行,互不联通,形成安全防御中的"孤岛"[11]。在这种情况下,安全管理人员要熟悉各类安全产品知识,逐一配置和执行防护措施。当面对高饱和、多类型的新型网络攻击时,往往会存在不熟悉处置策略、操作繁琐等问题,从而延误防御时机。要解决这一问题,需要整合各类安全设备,形成一站式闭环管理的处置中心,以便在统一系统中高效集中地处置网络攻击。

1.3　强化省市联动协防

针对业务数据传输上下联动的需求,陕西省气象信息网络将防御重点放在了内外网通信上,对内网通信的防护相对薄弱。各市局由于安全防护力量相对有限,容易成为网络攻击的突破口,从而导致内网安全风险的蔓延。当省级安全管理人员发现攻击之后,往往只能被动采取措施,如紧急中断省市之间的通信,再通知各市局自行处置。然而,面对高饱和的新型网络攻击,这段响应时间已经足够攻击者在各市局之间实现横向移动,造成更大的损失。为解决这一问题,需要强化省市间的协防机制,联通省市间的监测设备和边界防御系统,实现设备联动和自动处置,从而充分发挥省级安全资源优势,加强薄弱环节。

2　安全态势感知系统设计实现

结合陕西省气象部门网络安全防护现状,采用"中心节点分析,边缘节点协同"的省市联动应用模式,研究设计了安全态势感知系统在全省气象信息网络的部署拓扑、逻辑架构和系统功能,从而保障对全省气象信息网络流量的统一感知,同时适应了市局资源受限的实际情况。

2.1　安全态势感知系统网络部署拓扑设计

安全态势感知系统由流量探针、接入设备、态势感知平台组成。其中,流量探针能够收集网络流量;接入设备上传日志数据并执行安全策略;态势感知平台是"安全大脑",对各类数据进行加工、分析,并提供可视化操作界面[12]。网络部署拓扑是系统采集控制全省气象信息网络流量的基础。网络部署拓扑设计目的是明确安全态势感知系统硬件设备的部署位置和联动方式,形成合理的拓扑结构。

陕西省气象信息网络可以分为省级网络和多个地市局自治域。省级网络根据功能可分为核心网络区、办公接入区、业务区、安全管理区。其中,核心网络区承担和互联网、地市局通信的功能;业务区部署各单位业务系统;安全管理区则部署了部分安全控制系统。根据是否和省级网络、互联网通信,地市局自治域可以分为核心网络区和业务区。按照不同功能区安全需求,设计安全态势感知系统网络部署拓扑,如图 1 所示。

(1)核心网络区流量监测:鉴于实现网络攻击的主要途径有外部攻击和横向移动两种,将流量探针部署在省级网络和地市局核心网络区的核心交换机上,实现对内外流量、横向流量的采集。同时,为避免改变原有网络拓扑可能造成单点故障、性能瓶颈的问题,流量探针采用旁路部署的方式接入,无侵入式的镜像流量数据,上传到态势感知平台。

(2)态势感知平台部署:态势感知平台是安全态势感知系统的核心硬件,需要避免自身遭受攻击,以确保系统的稳定运行。因此,将态势感知平台部署在访问控制更为严格的安全管理区,只有授权的 IP 才能访问态势感知平台。

(3)联动多类型防火墙:联动全网防火墙可以在检测到攻击流量后实现实时阻断,避免发生安全事件。目前应用的防火墙包括传统防火墙和网站应用级入侵防御系统(web application firewall,WAF)[13]两类。其中,传统防火墙部署在互联网边界路由器、省市边界路由器、业务区,用于保护内部网络和业务系统;WAF 则部署在业务区,精细化地保护重点业务系统。通过设置防火

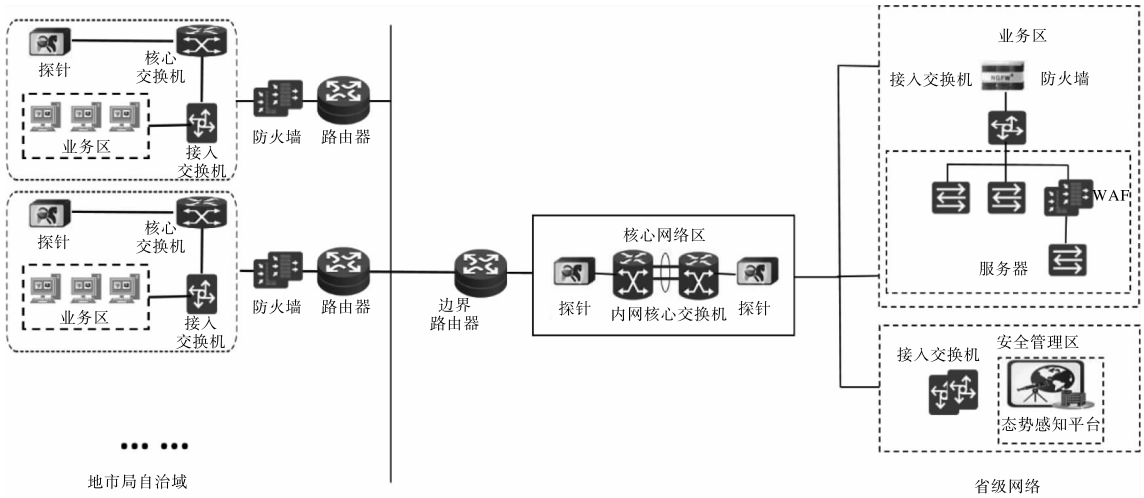

图 1 陕西省气象信息安全态势感知平台网络部署拓扑图

墙 IP、登录 URL、版本、设备密钥、管控类型等参数，可以将防火墙接入态势感知平台。同时，在态势感知平台为不同类型攻击设置静态 IP 阻断、动态 IP 阻断、域名阻断、DNS 请求拦截、病毒隔离等安全策略。当态势感知平台收到处置命令后，会自动匹配攻击类型和安全策略，实现精准处置。

2.2 安全态势感知系统架构设计

安全态势感知系统架构可以分为威胁情报(云端)数据库、数据采集层、存储计算层、核心分析层、用户感知层，如图 2 所示。

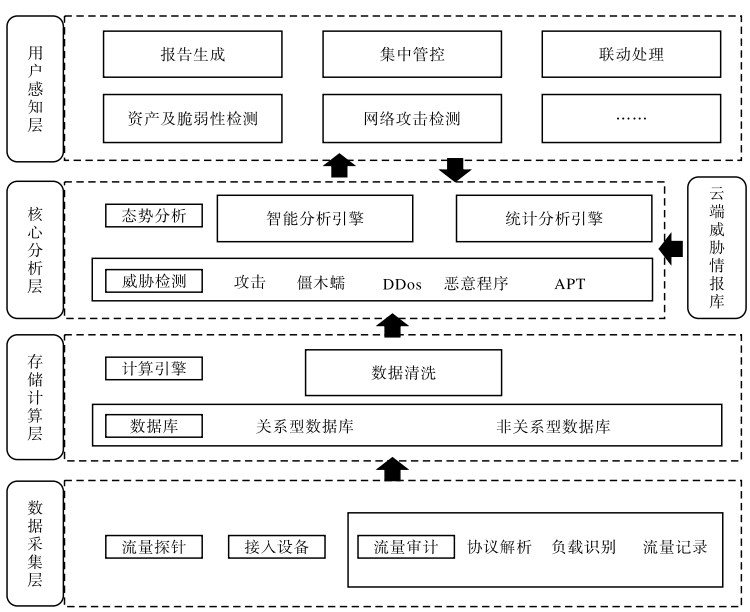

图 2 陕西省气象信息安全态势感知系统架构设计图

威胁情报(云端)数据库搜集存储了大量安全数据，包含 DNS 解析记录、IP 域名详情、病毒样本等内容，为核心分析层提供分析依据。

数据采集层首先通过部署的流量探针采集数据，将采集到的网络流量、日志等信息镜像发送到态势感知平台；然后通过流量审计模块解析 HTTP、SMTP、FTP 等文件传输协议、识别负载内容，获取完整的网络流量信息；最后对进出流量信息进行记录，为后续溯源取证提供数据支持。

存储计算层采用流处理引擎对采集的数据进行去重、处理缺失值、标准化数据格式等清洗操作，形成高质量的数据；之后存储到数据库中，为核心分析层提供完整、规范的网络流量信息。

核心分析层负责从海量数据中提取有价值的

安全信息,包含威胁检测模块和态势分析模块。威胁检测模块内置了攻击检测、僵木蠕检测、DDoS 检测、恶意程序检测、虚拟沙箱、APT 检测等检测引擎,可以从数据中发现网络资产(终端和服务器)、僵尸主机、木马病毒、APT 攻击等。统计分析引擎和智能分析引擎会采用统计和机器学习方法对威胁检测结果进行深度分析,从而评估网络攻击的行为类型、风险等级、攻击链条,为用户提供更深入的分析结果。

用户感知层提供了图形化操作界面,实时展示攻击检测和风险评估结果,支持用户决策。

2.3　安全态势感知系统功能设计

安全态势感知系统提供的功能如图 3 所示,包括资产及脆弱性感知、攻击检测、联动处置、报告生成、集中管控。

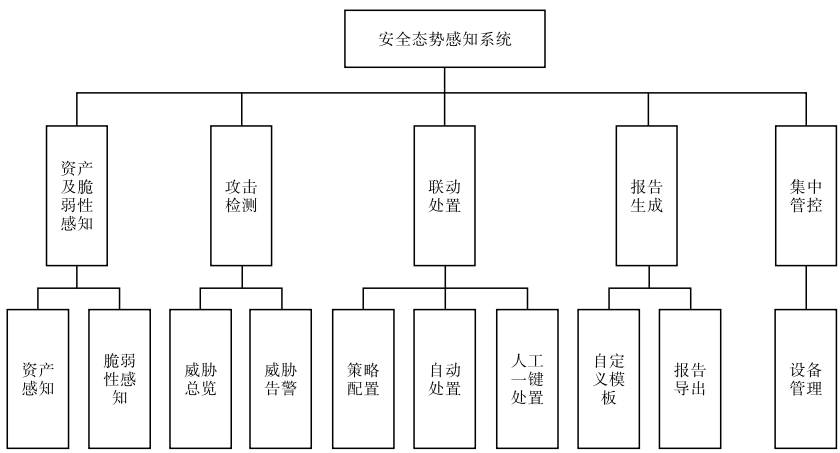

图 3　陕西省气象信息安全态势感知系统功能设计图

资产及脆弱性感知分为资产感知和脆弱性感知。资产感知是指发现活跃在网络中的主机、服务器等网络资产,将其按照用户划分的网段入库管理。脆弱性感知是指结合威胁情报量化系统漏洞、开放端口、防护软件数量等信息的风险,采用机器学习算法对入库网络资产的安全等级进行自动化的评估,从而将网络资产分为失陷资产、高危资产、中危资产和低危资产 4 类。

攻击检测是实时监测网络状态、识别网络攻击,包括威胁总览和威胁告警。威胁总览指以大屏、图表形式实时显示网络资产风险等级、遭受的攻击威胁等概况信息,帮助用户了解整体网络安全状态。威胁告警是指以列表形式实时显示受到的攻击威胁详情,内容包括告警类型、风险等级、源地址、目的地址、处置状态等,涵盖命令注入、SQL 注入、普通木马、FTP 暴力猜解、挖矿病毒等攻击方式。

联动处置包括自动处置和人工一键处置两种方式。自动处置是指用户可以为各类攻击设置风险等级、频次阈值、处置策略。当某 IP 的攻击达到阈值后,平台会自动向对应的防火墙下发指令,执行处置策略,并向用户发送邮件、短信。自动处置可以弥补人工监测频率、覆盖面的不足,及时阻断攻击,防止安全事件的发生。人工处置是指用户可以在平台一键执行阻断命令,避免因切换防火墙、联络其他责任人的时间扩大安全事件的影响。

报告生成是指根据模板生成安全报告。系统提供了网络安全态势报告、资产风险报告、全网威胁报告等预设报告模板,也提供了自定义安全报告模板的功能。通过模板,用户可以快速导出个性化的工作报告,为全网用户提供分析决策,便于开展安全防护工作。

集中管控是指对流量探针、接入设备进行管理,包括新增、删除、查看设备接入状态、配置属性等。

3　安全态势感知系统联动效果

在 2024 年网络攻防演习期间,从 8 月 1 日到 8 月 30 日,部署安全态势感知系统对全省气象信息网络安全进行了 30 d 的应用测试,主要测试功能包括资产脆弱性感知、网络攻击检测以及应急联动处置。经过测试,安全态势感知系统在网络攻击监测、联动处置等方面表现效果较为突出。

3.1 资产脆弱性感知

终端资产检测出37台风险主机，其中失陷主机0台、高危主机2台、中危资产9台、低危资产26台；风险问题以弱口令、挖矿病毒为主。服务器资产监测出6台风险服务器，其中中危1台，低危5台；风险问题以弱口令、系统漏洞、危险端口为主。发现风险资产后，用户迅速联系责任人，采取阻断恶意IP、更新口令、升级系统、关闭危险端口的措施，将中高风险资产全部降为低风险资产。

3.2 网络攻击检测

网络攻击检测共检测到21.5万条威胁告警，排除无效弱口令和正常的远程控制、建立通道操作后，还有2.01万条威胁告警，包括木马、SQL注入、文件读取漏洞攻击、命令注入、WEB扫描、跨站脚本攻击、暴力猜解等攻击类型，普通木马及SQL注入攻击数量占攻击总量的60%左右。

攻击路径方面，由内到外发起的外联威胁约0.8万条，外部威胁约0.91万条，横向威胁约0.3万条。经系统分析，外联威胁主要是由安装恶意软件感染挖矿病毒、勒索病毒、远控木马造成；外部威胁主要由攻击者通过SQL注入、命令注入、网页扫描、目录遍历、木马病毒等方式发起；横向威胁主要是因业务系统开发时未对用户输入、上传文件进行合规验证，当用户输入包含敏感字符、SELECT等数据库操作语句、可执行文件后缀时安全态势感知系统误报造成。针对以上威胁，采用部署天擎杀毒软件、阻断恶意IP、安装补丁、关闭旧业务系统等方式开展治理，治理后威胁告警由前10 d内13 760次下降为后10 d内3 276次。

3.3 应急联动处置

制定好联动策略之后，攻击威胁达到阈值后系统立刻生成动态访问控制列表，或由用户一键进行阻断。经统计，30 d内每日主动阻断恶意IP、域名、文件和发件域总个数在25个以内。其中，通过省级网络防火墙阻断威胁连接192个，联动地市局防火墙阻断威胁连接170个，处置时间均未超过半分钟。通过这样快速的处置方式，保证了2024年度网络攻防演习平稳过渡。

4 结语

针对陕西省气象信息网络的安全现状及需求，基于安全态势感知技术，研究设计了安全态势感知系统，开展了应用测试及分析。结果表明：该系统能够感知网络中的资产风险、威胁攻击，并联动省市防火墙快速处置网络攻击，有效提高地市局网络安全防护能力，保障气象信息网络安全可靠。后期，安全态势感知系统将接入更多安全设备，丰富监测对象和处置手段，为保障全省网络安全防护工作提供强有力的支撑。

参考文献：

[1] 吴寒，李晓东，成星恺，等．APT攻击检测技术研究综述[J]．通讯世界，2024，31(2)：61-63.

[2] 李昕雨，徐杨子凡．新型网络攻击安全防御策略设计[J]．网络安全技术与应用，2023(9)：20-22.

[3] 朱尧．网络安全态势感知问题研究：基于大数据背景[J]．网络安全技术与应用，2024(11)：20-22.

[4] 王克良．基于大数据的网络安全态势感知系统设计[J]．中国新通信，2024，26(21)：31-33.

[5] 杨志琼，牟舵．珠江委网络安全态势感知平台设计与应用[J]．水利信息化，2022(2)：16-20.

[6] 呼亚杰．农业农村部网络安全态势感知监测分析平台设计与实现[J]．农业大数据学报，2023，5(1)：68-75.

[7] 黄艳红，徐晓庆，岳勇，等．宁夏气象信息网络安全态势感知平台规划设计[J]．长江信息通信，2022，35(8)：57-60.

[8] 马晋，赵思亮．态势感知在气象网络安全防御中的应用[J]．微型电脑应用，2023，39(7)：13-16.

[9] 李宏存．省级收费公路联网收费系统网络安全态势感知平台设计研究[J]．中国市政工程，2022(2)：78-81.

[10] 徐枫，刘征，邱黎．广电业务支撑系统应对新型网络安全威胁的思考[J]．现代电视技术，2022(3)：127-129.

[11] 闫春旺．态势感知技术在气象网络安全中的应用[J]．网络安全和信息化，2023(3)：104-107.

[12] 鞠海斌．广电网络安全态势感知平台技术研究与应用[J]．广播与电视技术，2024，51(1)：118-122.

[13] 工业和信息化部．IPv6网络安全设备技术要求 第2部分：Web应用防护系统(WAF)：GB/T 44810.2—2024[S]．2024.