文章类型：论文|刊号（ISSN）：2737-4505(P) / 2737-4513(O)

基于网络安全态势感知的主动防御技术研究

付立平　王恩喜　刘锦宏
青岛特殊钢铁有限公司
DOI:10.32629/etd.v6i11.17503

[摘　要] 随着网络攻击手段日益复杂,基于网络安全态势感知的主动防御技术研究愈发关键。本文聚焦基于网络安全态势感知的主动防御技术研究。首先阐述网络安全态势感知的定义、发展、内涵与功能,接着剖析其关键技术,涵盖数据采集、预处理、融合、评估及预测等方面。随后探讨该技术在主动防御中的具体应用,包括实时监测预警、威胁情报分析、安全策略优化以及安全事件溯源与取证。最后展望其发展趋势,呈现智能化与自动化、云化与服务化、协同化与共享化等方向,旨在为提升网络安全主动防御能力提供理论支持与实践参考。
[关键词] 网络安全态势感知；主动防御技术；关键技术；应用；发展趋势
中图分类号：TP393.08　文献标识码：A

Research on Active Defense Technology Based on Cybersecurity Situational Awareness

Liping Fu　Enxi Wang　Jinhong Liu
Qingdao Special Steel Co., Ltd.

[Abstract] With increasingly sophisticated cyber-attack methods, research on active defense technology based on cybersecurity situational awareness has become increasingly critical. This paper focuses on the study of active defense technology based on cybersecurity situational awareness. It begins by elaborating on the definition, development, connotation, and functions of cybersecurity situational awareness, followed by an analysis of its key technologies, covering data acquisition, preprocessing, fusion, assessment, and prediction. Subsequently, it explores the specific applications of this technology in active defense, including real-time monitoring and early warning, threat intelligence analysis, security policy optimization, and security incident traceability and forensics. Finally, the paper looks into its development trends, highlighting directions such as intelligence and automation, cloudification and service-oriented transformation, and collaboration and sharing, aiming to provide theoretical support and practical references for enhancing proactive cybersecurity defense capabilities.
[Key words] Cybersecurity Situational Awareness; Active Defense Technology; Key Technologies; Application; Development Trends

引言

在数字化浪潮迅猛发展的当下,网络空间已成为国家、企业及个人活动的重要领域。然而,网络攻击手段日益复杂多样,传统被动防御模式难以有效应对,网络安全形势愈发严峻。网络安全态势感知作为一种新兴的网络安全理念与技术,能够全面、实时、准确地掌握网络空间的安全状况,提前感知潜在威胁,为主动防御提供有力支撑。研究基于网络安全态势感知的主动防御技术,对于提升网络安全防护水平、保障网络空间安全稳定运行具有至关重要的现实意义,将对此展开深入探讨。

1 网络安全态势感知概述

1.1态势感知的定义与发展

态势感知起源于军事领域,是对战场环境中敌我双方兵力部署、行动意图及战场态势变化等要素的全面感知与理解,以辅助指挥决策。随着信息技术发展,其概念延伸至网络安全领域。网络安全态势感知是对网络空间中各类安全要素,如资产状况、漏洞信息、攻击行为等进行动态收集、整合与分析,从而准确把握网络安全整体态势。从发展历程看,早期依赖人工简单监测,后逐步引入自动化工具。

1.2网络安全态势感知的内涵与功能

网络安全态势感知内涵丰富,它聚焦网络空间,全面收集涉及安全的各类数据,涵盖网络设备、应用系统、用户行为等多方面信息。通过对这些海量数据的深度挖掘与分析,清晰呈现网络安全现状与变化趋势。其功能多样且关键,能实时监测网络运行状态,及时发现潜在安全威胁并预警；对安全事件进行评估,判

断其影响范围与程度；预测未来安全态势走向，为安全策略制定提供前瞻性指导[1]。

2 网络安全态势感知的关键技术

2.1数据采集技术

数据采集是网络安全态势感知的基础环节，其质量与全面性直接影响后续分析结果。它需从网络环境中的多个源头获取数据，包括网络设备，如路由器、交换机，它们记录着网络流量、连接状态等信息；安全设备，像防火墙、入侵检测系统，能提供安全事件、攻击特征等数据；还有各类应用系统，其日志包含用户操作、系统运行状况等内容。为确保采集的及时性与准确性，常采用多种采集方式。主动采集可通过发送特定请求获取设备信息；被动采集则监听网络流量，捕获相关数据包。同时，要兼顾采集的效率与对网络性能的影响，避免因过度采集造成网络拥堵。此外，不同设备和系统产生的数据格式各异，采集技术还需具备数据格式转换能力，将多样数据统一为标准格式，以便后续处理，为构建全面准确的网络安全态势模型提供坚实的数据支撑。

2.2数据预处理技术

数据预处理在网络安全态势感知流程中起着承上启下的关键作用。原始采集的数据往往存在噪声、缺失值、重复值等问题，影响分析的准确性。数据清洗是首要步骤，通过设定规则去除噪声数据，如异常的流量峰值、错误的日志记录等；对缺失值进行合理填充，可根据数据的相关性采用均值、中位数或基于模型的方法；消除重复数据，减少数据冗余。数据归一化处理将不同量纲的数据转换到统一范围，使各类数据在分析中具有可比性，例如将流量大小、攻击次数等数据映射到[0,1]区间。特征提取与选择也不可或缺，从海量数据中挖掘出对态势感知有关键影响的特征，去除无关特征，降低数据维度，提高后续分析的效率与精度，为准确评估和预测网络安全态势奠定良好基础。

2.3数据融合技术

数据融合技术能整合来自不同数据源、不同类型的数据，提升网络安全态势感知的全面性与准确性。多源数据具有互补性，网络设备数据侧重网络底层信息，安全设备数据聚焦安全事件，应用系统数据反映业务层面的安全状况。数据融合通过综合这些数据，消除单一数据源的局限性。融合方法多样，基于统计的方法利用数据的统计特性进行融合，如加权平均法，根据不同数据源的可靠性赋予相应权重；基于模型的方法构建数学模型，如贝叶斯网络，通过概率推理实现数据融合；基于人工智能的方法，如神经网络，可自动学习数据间的复杂关系进行融合。经过融合的数据能更准确地反映网络安全态势，为态势评估和预测提供更丰富、可靠的信息，帮助安全人员全面了解网络环境，及时发现潜在威胁。

2.4态势评估技术

态势评估是对当前网络安全状况的全面评价，旨在确定网络面临的安全风险等级与态势严重程度。它综合多方面因素，包括已发生的安全事件数量、类型、影响范围，网络资产的脆弱性，以及当前网络流量特征等。评估方法丰富，层次分析法将复杂问题分解为多个层次，通过两两比较确定各因素权重，进而得出综合评估结果；模糊综合评价法利用模糊数学理论，处理评估中的模糊性和不确定性，更贴合实际情况；机器学习方法，如支持向量机、决策树等，通过对大量历史数据的学习，构建评估模型，实现自动化的态势评估。准确的态势评估能为安全决策提供科学依据，帮助企业和组织合理分配安全资源，优先处理高风险问题，及时采取有效的安全防护措施，降低网络安全风险。

2.5态势预测技术

态势预测技术通过对历史和当前网络安全态势数据的分析，推测未来一段时间内网络安全态势的发展趋势，提前发现潜在的安全威胁。它运用多种分析方法，时间序列分析基于数据随时间变化的规律，建立数学模型，预测未来态势走向，如ARIMA模型可对网络安全事件的发生频率进行预测；机器学习中的回归算法，如线性回归、逻辑回归，能挖掘数据间的内在关系，实现态势预测；深度学习中的循环神经网络(RNN)及其变体，如长短期记忆网络(LSTM)，擅长处理序列数据，在网络安全态势预测中表现出色，可捕捉数据中的长期依赖关系。准确的态势预测能使企业和组织提前做好防范准备，制定针对性的安全策略，在威胁发生前采取措施，有效避免或减轻安全事件造成的损失，提升网络安全防护的主动性和前瞻性[2]。

3 网络安全态势感知在主动防御中的应用

3.1实时监测与预警

实时监测是网络安全态势感知在主动防御中的基础应用。借助数据采集技术，持续收集网络中的各类数据，涵盖网络流量、设备状态、用户行为等。通过对这些数据的实时分析，能及时察觉网络中的异常情况。例如，当网络流量出现突增或突减，可能暗示着存在网络攻击或设备故障；用户异常的登录行为，如频繁尝试登录、从陌生IP登录，可能表明账户面临被盗风险。一旦监测到异常，态势感知系统会立即触发预警机制。根据异常的严重程度和类型，以不同方式向安全人员发出警报，如短信、邮件、系统弹窗等。同时，系统会提供详细的异常信息，包括异常发生的时间、位置、涉及的设备或用户等，帮助安全人员快速定位问题。实时监测与预警能够及时发现潜在的安全威胁，使安全人员能够在威胁造成实际损害之前采取措施，将损失降到最低，为网络安全提供实时的保护屏障。

3.2威胁情报分析

威胁情报分析是提升主动防御能力的关键环节。网络安全态势感知系统收集来自多个渠道的威胁情报，包括内部网络监测数据、外部安全组织发布的情报、开源情报等。这些情报包含各种威胁信息，如已知的恶意软件特征、攻击者的攻击手法、漏洞信息等。通过对威胁情报的深入分析，能够了解当前网络面临的主要威胁类型和趋势。利用数据融合技术，将不同来源的情报进行整合和关联分析，挖掘出潜在的威胁模式和攻击链条。例如，通过分析多个攻击事件中的共同特征，发现攻击者可能利用的特定漏洞或攻击路径。基于这些分析结果，安全人员可以提前

制定针对性的防御策略,如修补相关漏洞、调整安全配置、部署特定的安全设备等,从而在威胁到来之前做好防范准备,增强网络的主动防御能力。

3.3安全策略优化

安全策略优化是网络安全态势感知在主动防御中的重要应用方向。网络安全态势感知系统持续监测网络环境和安全状况,收集大量的安全数据和事件信息。通过对这些数据的分析,能够评估当前安全策略的有效性。根据评估结果,对安全策略进行动态调整和优化。如果发现某些安全策略过于宽松,导致大量攻击能够绕过防护,就加强相关规则的严格程度;如果某些策略过于严格,影响了正常的业务运行,就进行适当放宽。同时,结合威胁情报分析的结果,将新的威胁特征和防御要求纳入安全策略中。通过不断优化安全策略,使安全防护体系能够适应不断变化的网络环境和安全威胁,提高主动防御的针对性和灵活性,确保网络系统的安全稳定运行。

3.4安全事件溯源与取证

安全事件溯源与取证是网络安全态势感知在主动防御中的事后保障措施。当网络安全事件发生后,态势感知系统利用其收集和存储的全面数据,包括网络流量日志、设备操作记录、用户行为数据等,开展溯源工作。通过分析这些数据的时间序列和关联关系,逐步追溯攻击的源头、传播路径和攻击手法。在溯源的基础上进行取证,收集和固定与安全事件相关的证据。这些证据可以用于法律诉讼、内部责任认定和安全改进等方面。取证过程需要确保证据的完整性、真实性和合法性。通过安全事件溯源与取证,不仅能够惩罚攻击者,维护网络空间的法律秩序,还能总结经验教训,发现安全防护体系中存在的薄弱环节,为进一步优化安全策略和加强安全防护提供依据,提升网络安全的主动防御水平[3]。

4 网络安全态势感知的主动防御技术的发展趋势

4.1智能化与自动化

未来,网络安全态势感知的主动防御技术将深度融合人工智能与自动化技术。智能化方面,借助机器学习、深度学习算法,系统能自动分析海量安全数据,精准识别复杂多变的攻击模式与潜在威胁,实现从被动防御到主动预判的转变。自动化层面,一旦检测到威胁,系统可依据预设规则自动采取应对措施,如隔离受攻击设备、阻断异常流量等,无需人工干预,极大提升响应速度与防御效率。同时,智能自动化还能持续优化防御策略,根据网络环境变化动态调整,构建更坚固的网络安全防线。

4.2云化与服务化

云化与服务化是重要发展趋势。云化使态势感知主动防御技术摆脱了本地硬件的限制,依托云计算强大的计算与存储能力,可处理更庞大的数据,实现更广泛的网络覆盖。企业无需大规模投入硬件设施,按需使用云服务,降低成本与运维压力。服务化则将态势感知功能以服务形式提供,用户可根据自身需求灵活选择服务模块,如威胁监测、风险评估等。专业安全服务提供商凭借其技术优势与丰富经验,为用户提供高质量、定制化的安全服务,提升整体网络安全水平。

4.3协同化与共享化

协同化与共享化将进一步强化网络安全防御。协同化强调不同安全设备、系统之间的协同工作,打破信息孤岛,实现数据互通与功能联动。例如,防火墙、入侵检测系统、终端安全软件等协同作战,形成多层次、全方位的防御体系。共享化则注重安全情报与经验的共享,企业、组织间建立安全信息共享平台,及时分享威胁情报、攻击案例与防御策略。通过协同化与共享化,各方能够整合资源、优势互补,共同应对日益复杂的网络安全挑战,营造更安全的网络生态环境[4]。

5 结束语

在网络安全威胁日益复杂多变的当下,基于网络安全态势感知的主动防御技术研究意义重大且迫在眉睫。通过对数据采集、分析、评估与预测等关键技术的深入探索,我们构建起了能实时洞察网络风险、提前预警威胁的防御体系。智能化、云化、协同化等发展趋势为其注入新活力,让防御更精准、高效、全面。未来,我们仍需持续创新,不断优化技术,提升对新型攻击的应对能力,筑牢网络安全防线,为数字世界的稳定运行、个人隐私保护以及国家安全保障提供坚实有力的支撑。

[参考文献]

[1]黄宇.基于大数据的网络安全态势感知技术研究[J].信息系统工程,2021(10):50-52.

[2]戴祥华,张苏炯.大数据网络安全态势感知中数据融合技术的研究[J].中国信息化,2020(04):81-82.

[3]汪茹洋,李鹏.试论大数据技术网络安全态势感知平台[J].科技创新与应用,2020(10):23-24.

[4]李景龙,孙丹,肖雪葵.基于大数据的网络安全态势感知技术研究[J].科技创新导报,2021,16(30):119+121.