基于安全态势感知在网络攻击防御中的应用

陆浩旋
顺德职业技术学院　广东佛山　712000

摘　要：在计算机网络技术体系中，安全态势感知模型以及软件系统的研发与应用，能够精准适配计算机网络中的攻击防御业务功能应用需求。基于安全态势感知技术的网络攻击防御系统，能够重塑各类网络攻击行为，并能够对本区域内的计算机网络安全漏洞进行脆弱性分析，从而呈现可视化的安全态势。本文将着重探究基于安全态势感知的网络攻击防御应用要点。

关键词：安全；态势感知；网络；攻击防御

Application of security situation awareness in network attack defense

Haoxuan Lu
Shunde Polytechnic, Foshan, Guangdong, 712000

Abstract: In the computer network technology system, the development and application of a security situational awareness model and software system can accurately adapt to the application requirements of attack and defense business functions in the computer network. The network attack defense system which is based on security situational awareness technology can reshape all kinds of network attacks, and analyze the vulnerability of computer network security vulnerabilities in the region, so it presents a visual security situation. This paper will focus on the application points of network attack defense based on security situational awareness.

Keywords: Safety; Situational awareness; Network; Attack defense

引言：

计算机网络环境中的安全风险因素相对较多，并且能够对各项数据信息资源的准确性和可靠性产生严重的威胁。因此在构建计算机网络安全监管体系的过程中，需要高效运用多源数据融合的网络安全态势感知模型和大数据处理分析方法，才能够进一步提升计算机网络的自动预警效率以及态势预测精确度，还能够充分保障计算机网络系统中各类虚拟资产的安全性。

1　安全态势感知技术概述

在计算机网络安全的相关行业领域内，安全态势感知技术以及数据模型的广泛应用，能够显著提升计算机网络空间的风险感知水平，并能够定向筛选安全漏洞问题和非法攻击行为[1]。安全态势感知技术能够在原有计算机网络架构的基础之上，对数据层、物理层、业务层以及网络层中的关键通信设施进行安全加密运算，还能够对去中心化的计算机网络拓扑结构进行安全审计以及漏洞扫描等基础系统操作。安全态势感知技术以及对应

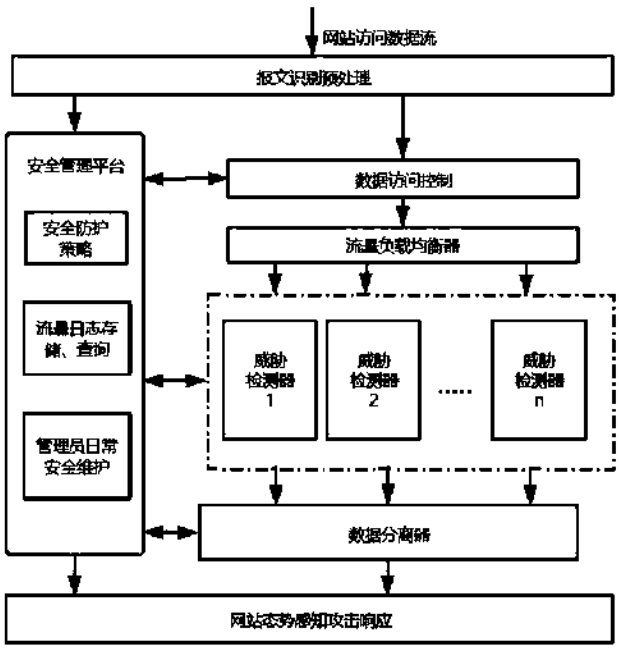

图1　网络安全态势感知技术框架

的数据模型，能够显著提升本区域内计算机网络的安全监测效率，并对异常状态下的数据源以及通信链路进行定量统计分析，快速识别和定位存在安全风险因素的网络通信链路编号等等[2]。但是在构建计算机网络安全态势感知系统的过程中，不可避免地会被较多不可抗力因素所干扰，但是也需要对不同等级保护机制的实际应用场合进行综合评估。充分借助于安全态势感知技术和数据模型，很多计算机网络架构体系中的安全风险评估结果会显著降低。

2 网络攻击防御中面临的问题

2.1 碎片化发展问题

对于不同规模的计算机网络安全防护技术体系，面对未知网络攻击的防御措施普遍存在较大差异，并且整体防护效果参差不齐。不同计算机网络节点上的被动防御模式普遍呈现碎片化的基本应用特征，也间接限制了较多安全感知模型的自动化运行效率[3]。很多去中心化的计算机网络架构体系，普遍应用三层攻击防护技术体系，但是不能够完全还原非法攻击目标和来源，也会间接产生较多潜在的安全风险因素。很多网络攻击事件越来越隐蔽，传播途径和通信链路更难被跟踪和溯源，因此碎片化的网络攻击行为不利于提升本地网络的整体防护和防御水准。碎片化发展的计算机网络攻击防御技术体系，并不能严格按照相关技术规范和标准的相关要求进行精准溯源，也会呈现离散化以及去中心化的网络技术发展趋势。除此之外，很多计算机网络从业人员并未严格审核各项非法攻击防御系统的精准度，理论与实践层面普遍存在较多脱节和断层问题，从而增加计算机网络的安全监测风险系数[4]。

2.2 被动拦截问题

在众多计算机网络攻击防御模型中，被动拦截的问题仍然比较普遍，并且能够间接影响到各类网络非法访问以及后台攻击行为的精准溯源，也并不能快速进行加解密运算，错过最佳的拦截时效。尤其在对计算机网络系统操作日志进行备份管理的过程中，会对各类被动拦截操作模式产生一定影响，也并不能完全匹配安全态势感知模型的内部数据信息资源，很容易呈现不稳定的预测分析状态，对网络攻击行为的反应灵敏度也会显著降低[5]。尤其在设定网络白名单和黑名单之后，被动拦截问题更加普遍，并且也会接连造成不可挽回的损失，对计算机系统设备和网络监控节点的稳定运行状态产生严重的影响。被动拦截问题不仅能够体现在网络攻击防御等技术层面之上，也会对各类安全监控设施的正常数据信息采集过程产生一定干扰。

2.3 单点防御问题

市面上网络安全相关的产品以及硬件设施种类和数量都相对较多，但是不能够精准适配计算机网络的差异化攻击防御需求。单点防御问题是很容易被忽略的计算机网络安全风险因素之一，并且能够间接影响到网络数据通信连接过程的精准性和安全有效性。在构建单点防御技术体系的过程中，需要尽量打破不同运营商之间的信息壁垒和安全规范不一致等障碍问题，才能够快速执行下一步信息共享和多源数据融合等基础操作。尤其在确定某项攻击防范措施之后，需要对单点防御过程中的各项技术性风险和经济性风险进行客观研判和预测分析，才能够进一步界定本区域内计算机网络架构体系中的潜在安全风险级别。运营商网络均处于各自为政的状态，能够实现的网络安全防御效果只是单点式防御。因此在处理单点防御问题的过程中，不能够忽略离散型网络安全监测数据信息之间的关联性，也需要重点识别和判断是否影响到不同数据通信链路的安全链接状态。

2.4 攻击结果未知问题

在网络攻击结果未知的情况下，管理人员无法对最终网络攻击结果进行预测；在网络攻击结果已知的情况下，管理人员虽然可以通过识别攻击者的网络攻击状况进行预警和攻击拦截，但仍然没有办法攻击目标，判断目标攻击是否成功。很多经典的网络攻击防御模型，在识别和判断非法网络攻击行为的过程中，也容易产生较多误判信息，从而影响到网络安全管理人员的最终决策结果。尤其对于具备迷惑性的IP地址以及源代码而言，很多网络攻击的潜伏时间相对较长，破坏过程非常隐蔽，在攻击结果未知的条件下，很多被动防御方法不能够精准判断和识别需要额外保护的数据源以及系统设备，也会浪费较多网络数据信息资源。攻击结果未知的问题，不仅能够严重影响本地局域网络和互联网络之间的数据通信传输质量和效率，也会间接产生冗余数据等安全隐患因素，并且不能够精准识别和定位系统日志中的关键操作结果，也并不能快速判断和分析防御目标和对象。

3 基于安全态势感知的网络攻击防御模型

3.1 数据源选择和特征抽取

基于安全态势感知的网络攻击防御模型，需要对NSSA技术的数据信息源类别和数量进行精准识别和自动化判断分析，才能够进一步界定某测试网络环境中显性和隐性安全风险因素的数量和类别。在NSSA模型中，需要对服务、主机以及网络三个核心业务层面的数据源进行集中筛选，并将异构传感器设备和异构数据信息资源的对应关系进行关联分析，构造去中心化的关联规则矩阵。为保证数据网络的多样性及完整性，必须利用数据多元融合方法对数据信息进行多元融合及实时处理，以

网络安全态势感知（NSSA）模型，然后在该基础上建立网络安全系统。在NSSA模型中，输入层、隐层、输出层的节点数量和特征值是非常关键的数据源，并且能够间接影响到各类异构安全感知设备的数据信息传输效率和安全性能指标。在应用BP网络和蚁群算法进行最优化选择的过程中，需要对特定的计算机网络安全测试环境和预测分析结果进行多维度训练和模拟预测，并将输出结果反馈给输入层进行校验训练。在进行特征选择的过程中，可以根据BP神经网络的三层数据传输架构，对节点数量和连续性函数进行统一选定，但是需要确保神经元中权重数值以及期望输出值的计算结果符合连续型函数的计算要求。

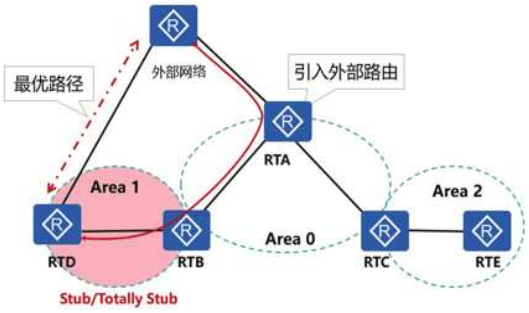

图2　NSSA的网络数据源

3.2服务安全态势感知

在构建NSSA安全感知模型的过程中，可以对不同感知层次进行量化分析，将服务层（业务层）、主机层以及网络层中的安全威胁因素进行定向分析和预测，并能够进一步界定本地网络服务的具体运行状态。在服务安全态势感知模块中，需要对非法网络攻击强度、攻击权重、攻击数目等自变量因素进行量化统计分析，也能够间接确定网络安全服务层面上的主动防御级别和溯源目标。除此之外，在对网络服务安全进行态势感知和定量统计分析的过程中，需要对自适应系数和学习速率进行适度调节，并定向调整网络攻击对应的防护等级。尤其对于大部分异构数据信息资源而言，在进行服务安全态势感知操作的过程中，不能够忽略业务服务层面的相关系统操作流程是否存在异常的控制节点和数据流，也需要对计算机网络的不同通信链路传输状态进行定向监测和统计分析。根据服务安全态势的感知和预测分析结果，计算机网络安全管理人员能够在可视化屏幕中定向调整后台防御等级，并对攻击数目和威胁权重系数等关键数据指标的变化趋势进行时间序列分析。在构建服务安全态势感知的BP网络模型过程中，需要对输出层的数据结果与隐层节点数目进行客观评测和定量分析。

3.3主机安全态势感知

在NSSA模型中，主机安全态势的感知数据结果非常关键，也能够间接影响到各项服务态势、服务数量以及比重系数的计算结果，在进行归一化处理之后，能够得出主机设备的网络安全威胁数据指标。在BP神经网络中，主机安全态势感知结果的输入层、隐层以及输出层都能够间接影响到网络服务的风险评估等级，也能够间接限定主机网络安全的被动和主动防御模式。但是在选定主机安全风险因素以及特征值的过程中，不能够忽略重要程度权重系数指标的相对一致性，也需要对安全威胁计算结果进行复核和正确性校验，以免影响到网络安全态势整体评估结果的精准度。

3.4网络安全态势感知

网络安全态势感知功能，需要与上述两种态势感知结果进行精准衔接，并将态势感知特征值以及主机比重系数进行精准计算。在计算网络安全态势感知结果的过程中，需要对重要程度权重数值进行归一化处理，对数据融合的高维度特征进行重点筛选。根据不同时间节点的网络安全态势走向图，需要对某个特定主机的服务个数以及时间序列分析结果进行精准判断和识别，并确保不同网络拓扑结构中的融合感知方法能够呈现系统兼容性，并对数据集中的训练数据和测试数据进行精准分类。在融合计算网络安全态势感知结果的过程中，需要对不同拓扑结构的计算机网络安全风险等级进行精准分类，并对感知结果的融合率、检测率、误警率进行归一化运算和统计分析，对不同数据源的事件检测取值范围进行统一界定。

4　结束语

随着网络空间安全重要性的不断提高，网络安全态势感知的研究与应用越来越得到关注。网络安全态势感知是一种基于环境的、动态的、整体的洞察安全风险的能力，网络安全态势感知的研究对于提高网络的监控能力、应急响应能力和预测网络安全发展趋势具有重要意义。

参考文献：

[1]刘俊红，张旗，韦文峰，姜春艳.人工智能在电力企业网络安全态势感知中的应用[J].网络安全和信息化，2021（12）：126-130.

[2]李程雄.网络安全态势感知系统关键技术研究[J].电子技术与软件工程，2021（23）：231-233.

[3]卢腾，胡威，程杰，崔兆伟，刘玉宽，张振山.基于OODA环的网络安全态势感知平台[J].信息记录材料，2021，22（12）：206-208.

[4]周娟.基于大数据的网络安全态势感知关键技术研究[J].电脑知识与技术，2021，17（31）：51-52+59.

[5]张小飞，张道银，郑珞琳，陈德成，付蓉.基于机器学习算法的电力信息网络安全态势感知研究[J].电器与能效管理技术，2021（08）：16-23.