基于态势感知理念的交通运输网络安全体系构建

文 / 黄祯晨 任逸飞 华东交通大学 江西南昌 330000

【摘要】 随着各行业对网络安全重视程度越来越高，态势感知作为一种新技术开始应用于网络安全领域。其结合大数据技术，能够全面感知网络安全态势、洞悉网络健康状态、实现溯源取证。作为信息化、数据化、智能化深度应用的典型行业，交通运输行业在国民经济中具有重要的战略地位，这也就意味着随时面临网络安全威胁，网络安全态势感知技术是解决这一问题的有力工具。本文将对交通运输行业网络安全形势进行全面分析，并提出适用于交通运输行业的基于态势感知理念的网络安全体系构建方案。

关键词：态势感知理念；交通运输行业；网络安全体系

在国家和行业信息化发展的背景下，物联网和智能化等新型信息化技术不断向各个行业渗透，交通运输行业也将进入全面联网、智能应用、业务协同的新阶段[1]。交通运输行业的全面联网也将面临黑客攻击、病毒侵扰、数据泄露、信息篡改等问题，对行业网络安全工作的开展提出了严峻挑战。

一、国内互联网安全背景和交通行业网络安全问题

随着信息化在各行业的推进，网络安全成为国家和各个行业不得不面对的重要问题。交通运输行业的发展关系到国家战略的实施部署，以及社会民生的发展和改善，也面临着严重的网络安全问题。

1. 病毒攻击长期存在

计算机网络病毒具有隐蔽性强、潜伏期长、传播速度快等特点，一旦被感染不易被发现，成为最大的网络信息安全隐患。交通运输行业感染计算机病毒将会进行链式传播，造成计算机系统瘫痪，如果不能及时发现并采取有效措施，将会严重影响交通运输效率、应急保障能力，为社会带来不便的同时，还会给国民经济造成严重损失。

2. 网络操作系统存在漏洞

网络操作系统是在信息化技术发展和实际工作需求的推动下不断迭代完善的，这也就意味着网络操作系统会具有滞后性，导致网络操作系统会存在一些固有的缺陷和漏洞。在交通运输行业，比较常见的缺陷和漏洞包括端口设置不科学、管理策略难落实、账户管理不到位等。

3. 资源共享存在安全隐患

在行业内进行有效的信息资源共享，是网络信息化的一大优点。但是，资源共享也具有两面性，既能够为人们生产生活带来方便，也成为一些不法分子窃取信息、篡改信息、破坏信息的主要渠道。由于交通运输行业在国民经济中具有战略性地位，成为国内外不法分子重点关注的领域。

4. 管理手段与信息化技术发展相脱节

网络信息安全管理区别于旧有的管理模式，由于网络信息化发展时间不长，很多人员的管理思维还未能转变，对网络信息安全认识不足，经常会套用或沿用旧有的管理手段进行网络信息化安全管理，不能严格按照操作规范及时排查潜在隐患[2]。在交通运输行业，除了管理思维和方法落后外，普遍存在相关人员综合素质不足、专业水平不够的情况。

二、基于大数据平台的网络安全态势感知系统

网络态势是指在整个网络中的所包含的各种用户行为、网络行为、网络设备运行状况等当下状态和发展趋势。网络安全态势感知指建立影响网络态势影响模型，全面、动态提取当前网络环境中的相关因素指标，对相关因素指标进行理解和分析，以此为基础预测网络状态的未来变化趋势。基于大数据平台的网络安全态势感知系统是通过大数据存储来自于网络数据流中采集到的数据，包括实时捕获、跟踪记录与检测、会话统计、协议处理分析等，将这些数据在大数据平台中进行预处理和建模分析，得出具有策略指导意义的数据信息，并以此为依据评估当前网络状态和预测后续网络环境中的威胁、预警和趋势预测[3]。基于大数据平台的网络安全态势感知系统通过多检测引擎机制，监测网络上的恶意代码的网络传播、网络病毒活动、网络攻击、网络劫持等各种网络安全事件。

1. 数据资源

数据资源包括第三方样本、DNS基础数据、自由样本数据、恶意URL数据形式组成的可用于大数据分析的数据信息，涉及到基础数据、知识数据、动态数据等内容。

2. 安全工具

安全工具是指在网络安全态势感知系统的基础上，提供针对各类威胁的检测结果、资产信息与日志的数据源的采集引擎、采集探针和采集程序。安全工具主要包括：未知攻击检测探针、异常行为检测探针、网络攻击检测探针、网站安全监测引擎、邮件安全监测引擎、资产扫描引擎、脆弱性扫描引擎、设备故障监测设备、日志采集工具、恶意代码检测工具、信息外泄检测工具等[4]。

3. 大数据分析平台的构建

大数据分析平台是对采集到的安全数据进行存储和处理的系统。交通运输行业网络安全大数据平台是指以行业关键信息基础设施为监测对象，将收集到的与网络安全相关的数据资源统一存储到大数据平台中，形成原始数据库；再将原始数据库中冗余的数据信息，进行预处理和特征提取，具体包括清洗、去重、转换、有效性验证、过滤等过程，最终完成存储和索引[5]。大数据分析平台通过多种数据计算引擎为不同场景提供数据处理结果，计算引擎包括：搜索、关联分析、统计、威胁监测等。

三、交通运输行业信息安全体系构建

1. 建设原则

交通运输行业动态感知安全系统建设需要遵循以下五大原则：（1）系统完整性原则，完整的安全体系能够有效防止不法分子有机可乘，保障系统安全。（2）系统实用性原则，具有有效性及可用性的系统才能够避免做无用功。（3）投入产出平衡原则，保证安全目标与效率、投入之间保持平衡，避免浪费。（4）系统动态发展原则，安全防范体系的建设需要在使用过程中不断完善和升级。（5）利旧原则，尽量通过采集已有设备数据信息完成态势分析，避免新的资源投入。

2. 建设目标

通过态势感知系统，对交通运输行业网络进行有效的防护，充分了解网络的整体安全状况，为信息安全策略提供有效依据。首先，实现交通运输行业动态感知安全系统目标，需要对关键节点进行实时监测，日常对系统进行安全漏洞扫描，一旦发现系统薄弱环节、恶意的入侵行为或者病毒传播，立即发出警报并推送给系统管理方。接下来，随着系统的不断迭代升级，从关键阶段的保护扩展到多个重点系统，全面确保阻止入侵行为的发生；同时对入侵行为进行分析，发现易受攻击的时间及子系统，重点加强子系统和相应时间段的安全防护。

3. 架构总览

系统分为数据采集、大数据处理和分析交互三层。

（1）数据采集层。使用部署在网络关键节点的引擎、探针和程序，监控行业服务系统的漏洞、系统配置问题、安全事件、病毒、木马等安全威胁，并采集这些威胁数据。数据采集到的数据可以分为高频数据和低频数据两类：高频数据，指通过高速数据总线收集到的数据，由于其具有速度快、数量大、异构性也称大数据，大数据主要包含系统状态和设备性能信息

及事件、日志和流数据等[6]；低频数据，指通过低频数据总线采集到的数据，主要包括资产信息、配置信息、人员信息、漏洞信息和威胁情报等。

此外，根据采集位置还可以将数据类型分为内部数据和外部数据两类：内部数据，采集于内网，通常包含网络安全数据、漏洞信息、员工审计信息等；外部数据，采集于互联网出口，一般包含外部威胁等信息。

（2）大数据处理层。将采集到的海量数据进行系统的归类和转化，将异构数据转化为结构化的大数据集，不能进行结构转化的数据进行标签化，添加索引。再将两种转化后的数据进行存储，用于后续交互分析。

（3）分析交互层。分析交互层分为安全监测、态势分析、漏洞预警、事件分析四个模块。

安全监测。安全监测模块是系统整体的安全防护体系的基础，对网络上的重点系统、重点目标及重点人员进行专项监测，对网络及系统的状况进行整体监测。该模块既能够监测外部系统对内的威胁信息，还能够监测并警告内部组织或人员对外部网络的攻击。同时，为了减轻服务器负担和维护人员工作量，系统还可以对不重要的入侵及攻击事件进行智能过滤筛选。安全监测模块可以对特定时间段内的安全事件进行对比分析，并形成的分析报表，便于使用者对系统安全进行直观了解。

态势分析。态势分析模块包含宏观分析和微观分析两大方面：宏观分析，以互联网总体信息安全状态入手，宏观展示整个网络的安全威胁；微观分析，对重点人员和系统进行详细的分析，重点展示主要目标的威胁态势和安全态势。

漏洞预警。漏洞预警模块日常对系统数据进行全面的检测，系统漏洞和各种弱点，并提前预警并协助用户及时填补漏洞，提前感知可能遭受的威胁。

事件分析。事件分析模块通过对已发生的安全事件进行汇总分析，协助使用者找出重点威胁事件、攻击源头及重点对象。

分析方法通常为三元组分析、异常服务分析和攻击者分析。其中，三元组分析是将攻击事件行为、源IP和目的IP进行统计分析。同时，系统还可以就异常服务和参与对外攻击的主机进行分析，挖掘疑似攻击人员信息。

4. 安全评估

网络安全评估系统利用大数据平台构建风险评估模型，对重点监测对象的资产信息（安全设备、网络设备、数据库、操作系统和应用中间件等）、脆弱性（网络结构脆弱性、应用系统脆弱性、系统软件脆弱性、应用中间件脆弱性等）、威胁数据（操作失误、越权或滥用、泄密、恶意代码、篡改、网络攻击等）进行漏洞扫描，将扫描到的漏洞信息通过风险评估模型进行风险分析，全面评估整个系统的安全风险，并将相应的安全风险评估结果展示给相关负责人[7]。

安全评估可分为三个部分：构建评估模型、系统漏洞扫描、威胁评估分析。系统面临安全风险的直接原因是系统存在安全漏洞。系统漏洞扫描部分分为漏洞信息收集、扫描漏洞和结果评估三个步骤。通过对大数据平台中收集的漏洞信息进行模型测算分析，可以得出系统当前的安全风险值。

参考文献：

[1]刘世栋.基于大数据的网络安全态势感知平台构建[J].保密科学技术,2019(6):47-51.

[2]许暖,刘洋.关于网络安全态势感知体系及关键技术的思考[J].中国新通信,2020,v.22(20):133-134.

[3]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].科学与信息化,2020(31):37-37.

[4]柯宗贵,杨育斌,麦思文.基于大数据的网络安全态势感知解决方案[J].信息技术与标准化,2019(9):21-22,45.

[5]潘振航.江苏省交通运输网络安全综合监管平台的建设研究[J].科学与信息化,2020(21):151-151.

[6]才让昂秀,郭玉明,李慧禎.青海交通运输行业网络安全管理浅析[J].企业科技与发展,2020(9):222-223.

[7]关伟、吴建军、高自友.交通运输网络系统工程[J].交通运输系统工程与信息,2020,20(6):9-21.