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

基于态势感知的电力行业网络安全预警模型构建

黄炳茜
大唐山西电力工程有限公司
DOI:10.12238/etd.v6i3.14367

[摘　要] 伴随信息技术的迅猛发展,以国家关键基础设施身份存在的电力行业,其网络安全态势感知的重要意义日趋明显。本文要探讨的是网络安全在电力行业态势感知中的功能,进而构建依托态势感知的电力行业网络安全预警体系,对预警指标的选取与归类进行了分析,且提出了对应的量化途径,拟定了预警模型的理论框架及算法实施,保障模型可高效识别并应对潜在网络安全威胁,采用模型验证及评估方式,保证预警模型的精准度和实用效能。本研究成果可推动电力行业网络安全管理水平的提升,维持电力系统的平稳运转。
[关键词] 网络安全；态势感知；电力行业；预警模型；信息安全
中图分类号：TM727　**文献标识码**：A

Construction of a Cybersecurity Early Warning Model for the Power Industry Based on Situational Awareness

Bingqian Huang
Datang Shanxi Electric Power Engineering Co., Ltd.

[Abstract] With the rapid advancement of information technology, the power industry, which is a critical national infrastructure, has increasingly recognized the importance of cybersecurity situational awareness. This paper explores the role of cybersecurity in situational awareness within the power industry and aims to establish a cybersecurity early warning system based on situational awareness. The paper analyzes the selection and classification of early warning indicators and proposes corresponding quantification methods. It outlines the theoretical framework and algorithm implementation of the early warning model, ensuring that the model can efficiently identify and respond to potential cybersecurity threats. The paper also employs model validation and evaluation methods to ensure the accuracy and practical effectiveness of the early warning model. This research is expected to enhance the cybersecurity management level in the power industry and maintain the stable operation of the power system.
[Key words] network security; situation awareness; electric power industry; early warning model; information security

引言

处于数字化转型的浪潮里,作为国家关键基础设施的电力行业,其网络安全事宜日益备受瞩目。网络安全态势感知,作为预防及应对网络攻击的关键手段,在保障电力系统稳定运转方面意义重大。基于此,本文聚焦于探究网络安全于电力行业态势感知里的作用,进而创建依托态势感知的电力行业网络安全预警模型。

1 网络安全在态势感知电力行业中的作用

网络与信息系统对发电企业的生产运营起着高度支撑作用,涉及设备监控、电力调度乃至数据管理等各个环节,均离不开网络作支撑,网络安全稳固与否的情形,关乎着电力系统能否平稳运转,若网络安全出现了漏洞,恶意攻击者或许会借机潜入,篡改控制指令、打乱通信,让电力设备陷入故障状态,甚至导致电网出现大面积停电,极大地威胁到电力系统的稳定与可靠运行,这在保障电力持续供应上极为关键。就推动社会经济稳定运作的角度而言,在现代社会里,电力充当基础性能源,与工业生产、交通运输、金融服务等诸多领域相关联,若发电企业碰到网络安全领域的事故,引起大面积的停电局面,必将使社会经济承受难以估算的损失,甚至有引发社会秩序紊乱之虞。

2 基于态势感知的电力行业网络安全预警模型构建

2.1预警指标体系构建

2.1.1预警指标的选择与分类

发电企业应使网络安全预警指标紧密围绕自身业务特性及安全需求,需留意发电机、变压器等关键电力设备的运行状态指标,诸如设备温度、振动幅度这类出现的异常变动,或许暗藏潜在风险；着重考量诸如网络流量速率、协议分布、异常连接数等指标,流量的异常波动或是大量未知协议连接,也许是网络攻击的先兆。与数据完整性和保密性相关的指标极为关键,诸如数据篡改的发生率、敏感数据的泄露潜在危机等,将目光聚焦于电力生产控制系统应用的可用性、漏洞数量等指标层面,以性质为依据分类,可归为实时运行指标、安全威胁指标、脆弱性指标等类别。实时运行指标显示设备与系统的当下情形；安全威胁指标标示出外部攻击与内部违规操作的相关迹象；脆弱性指标凸显系统自身易被攻击的薄弱要点,凭借这般周全且针对性强的指标选择及分类,为发电企业网络安全态势感知打造精准的数据基石,为保障预警指标体系既科学又实用,需把各指标权重进一步细化。可借助层次分析法(AHP)和德尔菲法的联合,召集电力行业专家和网络安全领域技术人员,全面权衡指标对网络安全的影响大小、出现概率等要素,厘定权重系数,设立动态化更新机制。

2.1.2预警指标的量化方法

为使预警指标可在分析中有效运用,量化实属必要,就设备运行状态的指标而言,可凭借设备历史运行数据与技术规范,界定正常运行参数的合理区间,把实际监测值与该区间进行对照比较,用偏离程度对异常状况进行量化,就如设备温度超出正常范围上限值的占比。对网络流量指标实施量化时,采用统计分析手段,以历史流量数据为基础构建正常流量模型,采用像均值方差、移动平均的算法模式,算出当前流量对模型的偏离值,利用此对流量异常程度量化,与数据有关的指标,可采用计算数据校验错误率的办法量化数据完整性；在保密性这一范畴,依靠加密算法强度等级以及密钥管理规范程度等进行量化评定。以系统停机时间占总运行时间的比例对可用性进行衡量；直接从专业漏洞扫描工具检测结果里获取漏洞数量,依靠这些量化途径,把各类预警指标转变成能计算、可对比的数据,方便后续开展深度剖析与预警判断,对用户行为指标实施量化期间,可凭借分析历史操作数据打造正常行为模式,统计用户在登录频率、操作时长、权限使用次数维度上的均值及标准差,把实时行为数据同模式予以对比,以偏离阈值倍数对异常风险予以量化,如异常登录地点的访问频次出现陡然变化。就物理环境相关指标而言,可利用传感器直接实时采集温湿度、烟雾浓度等的数值,与设备安全运行相关标准阈值做对比,凭借绝对差值或者超标时长量化环境风险等级,如机房温度超出临界值的时长,在业务层面指标这一范畴,可借助设定资金流向偏离度、交易频次波动系数等量化模型,识别交易数据异常,辨识洗钱、欺诈等潜在威胁；衡量业务流程效率,可采用节点处理耗时平均值、超时率等参数,可采用机器学习算法,诸如孤立森林与LSTM的神经网络,实施多维度量化后指标的关联探究,实时动态调整各指标的权重,打造综合预警的评分体系,达成从单一指标监测向多维风险态势把握的升级过渡,增强预警的精确性与及时性。

2.2预警模型设计

2.2.1预警模型的理论框架

发电企业网络安全预警模型把态势感知理论当作核心,把信息融合、风险评估等理论融合以打造框架,态势感知承担实时采集、弄懂并预测网络安全状态的工作,信息融合理论把多源异构的预警指标数据作为处理对象,诸如设备传感器的相关数据、网络流量监测的有关数据、安全漏洞扫描的对应数据等,依靠加权融合、D-S证据理论等手段实行融合操作,去除数据存在的冲突,让数据可靠性与完整性增强。以融合后的数据为支撑,风险评估理论开展评估,评估网络面临的风险级别,判定安全威胁出现的可能性及其影响大小,采用攻击树模型、贝叶斯网络等作为分析工具,探究各安全事件出现的概率与事件间的因果关联,整个理论框架以数据采集、融合为开端,到风险评估与态势预测结束,造就闭环反馈的有效机制。伴随新数据接连不断地涌入,持续对模型参数及评估结果做优化,进而精准把握发电企业网络安全局势,给及时有效预警打造坚实的理论支撑体系,以上述理论框架作支撑,预警模型也引入了动态自适应机制,采用机器学习算法对历史数据进行深挖,分析网络安全态势转变的规律跟趋势,促使模型能适应发电企业网络环境的动态革新。

2.2.2预警模型的算法实现

就算法实现这件事而言,采用深度学习与机器学习算法契合,针对设备运行状态及网络流量开展异常排查,借助支持向量机(SVM)、孤立森林等机器学习算法开展相关工作,SVM借助探寻最优分类超平面,区别正常与异常的数据集；孤立森林依靠数据点在随机树的深度测定其异常程度。就数据安全与应用安全的复杂场景而言,采用如卷积神经网络(CNN)、循环神经网络(RNN)这般的深度学习算法,CNN擅长应对带有空间结构的数据,可借助分析数据文件特征检测数据是否被篡改；RNN可开展时间序列数据处理工作,适合对应用系统操作日志开展监测,找出异常操作行为的模式。利用如梯度下降的优化算法调整模型的参数,依靠大批历史安全数据对模型训练,令其熟悉正常及异常状态的特征模式,在实时运行的阶段中,将刚采集的预警指标数据投进训练好的模型,模型借由学习到的模式判断当前网络安全形势,给出实时预警等级,实现精准高效的预警效果。在模型的集成与优化阶段,借助Stacking集成学习框架汇聚多算法长处：把SVM跟孤立森林的输出用作底层特征,投入由CNN-RNN混合网络组成的高层模型里面,依靠门控机制(如LSTM/GRU)捕捉时空特征之间的关联,增强复杂场景下异常鉴别的精准度。采用迁移学习的策略,针对特定行业安全数据分布的差异化情形,借助预训练的模型为支撑,以小样本行业数据实施微调,既降低数据标注的成本,又提高模型的泛化能力,在工程部署这个维度,搭建分布式实时推理引擎：采用Flink流计算框架,把训练后的模型参数分布式存储在Redis集群,依靠Kafka消息队列实时摄取预警指标相关数据,由预处理模块完成标准化后,并行输入到模型集群,达成毫秒级响应的线上预警,配套构建模型健康监测体系,

对模型于生产环境中的预测准确率、特征漂移等指标进行实时跟踪,引发自动retraining动作,基于最新安全事件数据对模型实施动态更新,保证预警能力始终有效可行。

2.3预警模型的验证与评估

2.3.1模型的验证方法

为保障预警模型达到可靠水平,采用多样验证办法,起始为历史数据验证操作,采集发电企业过往某段时间内切实出现的网络安全事件和对应时间段的预警指标数据,把这些数据投进模型,把模型预警结果输出与实际安全事件进行对照比较,考查模型是否可精准辨别历史安全事件且在恰当之际发出预警。然后是模拟攻击验证相关工作,在模拟好的发电企业网络环境情形里,人为地引入各类常见网络攻击,诸如DDoS攻击、恶意软件渗透之类的,评估模型对模拟攻击的检测与预警水平,涉及预警的及时特性、准确特性,以及预警级别与攻击严重程度的契合度。其次要进行交叉验证,将收集的大量安全数据拆分为多个子集,采用像K折交叉验证这样的方式,每次采用不同子集作为测试数据集,把剩余部分用作训练集,对模型开展多次训练与测试,全面评价模型在各种数据子集的性能状态,防止模型出现过度拟合现象,全面确认模型于不同场景下的有效性。除已说明的这些方法之外,也可引入专家评估途径,邀请发电企业运维人员与网络安全领域专家组成评估小组,凭借专业素养对模型预警逻辑、风险判断依据等开展审查工作,专家基于行业经验与最新的安全走向,评判模型对复杂网络安全场景的适应情况以及预警策略的合理与否。

2.3.2模型的评估指标

评估预警模型挑选多维度的指标,准确性指标可对模型预测的预警结果与实际安全状况的符合度进行衡量,通过综合计算真阳性率(模型将实际正样本准确预测为正样本的比例情形)、真阴性率(模型将实际负样本准确预测为负样本的比例情形)等完成评估。及时性指标着眼于模型自安全威胁冒起到发出预警的时间间隔情况,较短的时间体现出模型响应的及时性越强,漏报率表示的是实际发生安全事件时模型未发出预警的比例,最好是漏报率降低;误报率反映模型错误发出预警所占的比例,越低说明模型精准程度越高。同样考量模型的稳定水平,于不同的时间段、不同网络负载等情况中运行模型,留意模型评估指标的起伏态势,若波动减小,就说明模型的稳定性提升,能在发电企业复杂且不断变化的网络环境里可靠运行,为网络安全预警筑牢坚实后盾,除了刚刚说的那些指标外,可把可解释性指标引入进来,采用SHAP值、LIME等方式对特征重要性加以分析,保证模型决策逻辑与发电企业网络安全业务的逻辑相适配,提升运维人员对预警结果的信赖感,同时把资源占用指标包含进去,对模型运行时的CPU消耗、内存耗用及响应延迟加以监测,保障其于发电企业现有硬件环境里实现高效部署,实现评估体系自“效果”至“效率”的全面覆盖。

3 结束语

总之,随着电力行业对网络安全方面要求的不断提高,于电力行业而言,态势感知技术的应用重要性渐趋凸显。本文提出的凭借态势感知的电力行业网络安全预警模型,依靠科学的预警指标体系及有效的算法达成,为电力行业供给了一种高效的网络安全管理手段。伴随技术持续革新与应用逐步拓展,此模型预期可进一步优化,为电力行业网络安全赋予更精确高效的预警服务。同时电力行业需始终关注网络安全技术的发展走向,加速网络安全人才培养步伐,以此保证电力系统安全稳定地顺利运行,为国家经济发展和社会稳定的良好局面增添更大功绩。

[参考文献]

[1]郭孝基,董彩红,王湘女.基于人工智能的网络安全态势感知系统设计[J].电子元器件与信息技术,2024,8(12):208-210+215.

[2]电力行业网络安全建设路径与实践[J].网络安全和信息化,2023,(07):37.

[3]国家能源局印发《电力行业网络安全管理办法》[J].自动化博览,2023,40(01):3.

[4]韩洁,钟逸铭,陈明亮.电力行业网络安全态势感知分析[J].软件,2022,43(05):128-130.

[5]黄剑祎,孙瑞瑞,李蒋俨.广播电视行业网络安全态势感知预警平台的设计与思考[J].广播与电视技术,2021,48(04):116-123.

作者简介：

黄炳茜(1993--),女,汉族,山西省太原市人,本科,工程师,从事信息通信技术、网络安全。