能源行业网络安全防护技术研究与展望

谭震
中海油信息科技有限公司北京分公司，北京 100000
DOI: 10.61369/TACS.2025120001

摘　　要： 能源行业数字化转型不断深入之际，网络安全成了限制其平稳前行的关键要素，本文着眼于能源行业网络安全保障的主要需求，全面探究网络安全关键技术的应用思路及其执行途径，面对当下网络攻击日益繁杂，内部经营存在风险，技术更迭造成安全隐患等问题，着重分析分层防护体系创建，防火墙及入侵检测防御，数据加密这些关键技术的原理以及适用场合，通过技术落实实例来归纳关键性技术于安全形成及运作期间所积累的实际操作经验，然后预测将来技术发展走向，给能源行业改进网络安全技术保护水准给予参照。

关 键 词： 能源行业；网络安全；关键技术；技术应用；发展展望

Research and Prospect of Cybersecurity Protection Technology in the Energy Industry

Tan Zhen
Cnooc Information Technology Co., LTD., Beijing Branch, Beijing 100000

Abstract: As the energy industry continues to deepen its digital transformation, cybersecurity has become a critical factor that hinders its smooth progress. This paper focuses on the primary needs of cybersecurity protection in the energy industry, thoroughly examining the application concepts and implementation methods of key cybersecurity technologies. In the face of increasingly complex network attacks, risks within internal operations, and security vulnerabilities caused by technological changes, the paper highlights the principles and application scenarios of key technologies such as layered protection systems, firewalls, and intrusion detection and defense, as well as data encryption. By summarizing practical experience gained through the implementation of these technologies during the formation and operation of security, and then predicting future technological trends, the paper provides insights for the energy industry to improve its cybersecurity protection standards.

Keywords: energy industry; cyber security; key technologies; technology application; development outlook

引言

能源产业成为国家战略层面的支撑力量，能源产业开展数字化进程之时，能源生产环节，能源输送环节，能源分发环节全都把网络系统融入其中，网络安全技术得到充分应用并且不断尝试新的发展道路，能源供应稳定与否，国家能源安全状况以及企业自身的关键利益紧密关联起来，能源行业面临网络攻击方式升级，物联网设备存在安全隐患，内部操作出现差错等情况，当前的安全防范措施已经不够用了，要探究网络安全关键技术的主要突破口，思考技术创建运作时怎样做到相互结合执行，明确能源网络安全保护工作所处的关键位置[1]。

一、能源行业网络安全技术应用的核心价值

（一）保障能源生产传输的技术可靠性

能源生产调控系统以及输电调度网络想要稳定运行下去，就要依靠安全技术来形成一道重要的防线，守护好那些关键设备和数据的安全，采用诸如加密手段，入侵防护策略之类的技术执行动作，从而把那些试图非法闯入或者改动数据的行为给堵住，保证能源方面的指令能够被精确地传达出去，而且在传送过程中的数据也是真实的，可以减少因为技术上存在破绽而造成生产突然停止或者调度出错的情况发生[2]。

（二）筑牢国家能源安全的技术屏障

自主可控技术重点的安全执行途径，属于抵御特定网络攻击的险关隘口，通过安全结构塑造，漏洞搜寻并修补等方法，开展核心技术机密数据外泄的防范举措，守护能源设施免遭专门打

击，给国家能源策略执行打造起一道技术安全保障墙。

（三）降低企业运营的安全技术成本

完备的网络安全技术布局，准确找到风险点并快速处理，利用自动化检测与智能化回应技术，减少人为干涉性开销，避免因安全事件造成设备损毁、资料丢失等损失，改善企业的运作效能及其安全方面的投资收益情况。

二、能源行业网络安全面临的技术挑战

（一）网络攻击技术迭代加剧防御难度

面对能源领域的数字化转型大潮，黑客攻击技术渐渐朝着“精确，隐秘，连续”这个方向发展，网络安全防卫遭遇严峻挑战，针对能源公司遭受的攻击状况展开讨论，那些已经知晓漏洞的攻击方法不再是单一形式，黑客利用逆向工程，模糊测试这些手段，发掘那些没有被公布过的“零日漏洞”，在战前展开长时间的侦察审理，针对能源公司的业务操作弱点来规划攻击路线，从而提升漏洞运用行为的隐蔽性门槛。恶意软件散播更具针对性，专门针对电力调度系统的勒索病毒会伪装成能源生产系统更新补丁或者数据收集程序，潜入到核心主机核心层，并带有隐藏以及横向蔓延的功能，可以逃过传统反病毒工具的检查，传统安全防护技术大多依靠既定规则及特征数据库，对于未知漏洞攻击的防御策略分析，很难快速察觉攻击迹象[3]。

（二）技术融合带来的跨界安全漏洞

能源产业正通过物联网，大数据，人工智能等技术达成融合，能源体系由“封闭隔绝”走向“开放互通”，网络边界的旧有特点慢慢消退，跨行业的安全漏洞急速增多，物联网技术应用的执行范围看，智能能源监测设备，比如电力系统的电流电压检测装置，油气管道的压力监测器，智能巡检机器人等等，由于成本和技术上的阻碍，无法全面采用，普遍设置预设的初级密码，没有安装安全加密模块，通信期间，大量使用未加密的 Modbus，DNP3等传统工业通讯标准，黑客可以凭借密码破解，通讯数据截获等方法展开攻击，针对传感器收集到的重要信息展开篡改，能源调配决策错误的原因考察和剖析。大数据技术对于能源负荷预测以及用户行为分析方面被深入挖掘之后，导致大量的生产资料还有用户隐私资料聚集保存于某些地区，如果大数据平台出现权限监管方面的漏洞情况时，黑客就会大量窃取这些私密的数据信息，能源系统的智能化程度提升同人工智能技术密切相关，但是也存在着算法方面的缺陷之处，黑客利用数据投毒或者模型规避之类的手段来干涉 AI 的决策过程，关于电力负荷预测模型训练数据遭到篡改的现象加以讨论，电网负荷调度陷入失衡状况之中，这些跨越技术界限的安全漏洞问题群集起来考虑，因为涉及到的设备种类众多而且数据流转路线比较复杂，所以传统的按照区域和设备类别划分的防护方法很难做到全方位防护的效果，面对着跨场景，跨设备的情形时，技术层面的防护就面临着很大的挑战[4]。

（三）现有技术体系的适配性不足

当下的许多能源企业群体当中，特别是一些中小型企业，仍然沿用着数字化变革之前的那种安全防护框架，这种设计把重点放在了“边界守御”之上，依靠防火墙，杀毒软件这些静态防护手段，很难适应如今的业务转型环境，分布式新能源电站和电网调度中心要随时进行数据对接，而传统的防火墙规则更新存在着时间延迟问题，无法应对频繁发生且数量庞大的数据传输安全威胁；能源公司推行的数据云化战略执行以后，传统的本地安全设置就很难再对云端的数据实施有效的防护措施，尤其关键的是，在技术实施方面存在着一种“重视创建而轻视运作”的老毛病，企业完成购买安全设备这一环节之后，并没有组建起专门的运营队伍架构，导致设备一直处在闲置状态，不能灵活地去应对外部不断出现的新危险情况，而且安全技术和业务系统的融合度也不够好，电力调度系统的安全防护部分同调度工作流程并没有做到联动，在系统察觉到可能存在安全隐患的时候，只能简单地阻止信息继续传送下去，从而造成调度工作的中断。传统技术体系缺乏动态调整以及迭代改良的途径，很难顺应能源业务拓展（譬如风电项目增添，用户涵盖面扩展）以及攻击技术发展步伐，迅速修正安全防护办法，最后掉入“守势防御”的困境，难以抵挡网络安全新挑战。

三、能源行业网络安全关键技术研究

（一）安全架构构建关键技术

分层防护架构技术：在能源网络安全防护系统中，网络安全防护架构技术针对网络边界、内部网络以及主机节点这三层实施防护措施，综合利用了诸如访问控制列表（ACL），虚拟局域网（VLAN），主机入侵防御系统（HIPS）之类的技术手段来构建起多层面互动式的防护体系架构，从网络边沿角度出发去执行新一代智能边界防火墙的安装步骤过程，这个系统可以依照预设好的规则精准地完成针对 IP 地址与端口的准确实施动作，并且能够加入即时威胁警报机制，在面对外部异常接入行为时马上予以封锁处理，像自动屏蔽那些已经被识别出来的恶意 IP 地址所发出的接入请求之类的操作；而当涉及到整个网络内部结构布局情况的时候，则会用到 VLAN 技术对于能源生产调度部门，客户服务部门这些单位所属的网络部分实施逻辑上的隔离操作，在这样一种设置之下即使某个 VLAN 区域内发生了被攻击破坏的事情也不会让这种状况蔓延到其他的网络区域当中去，从而有效地减少了横向攻击方面的风险存在可能性，实时追踪着内网里的各种数据流动情形，依靠着网络流量监测工具随时发现其中是否存在有异常的数据交换现象发生。主机节点视角界面上，各个服务器以及工作站这类设备上开展实时更新病毒库防护系统的设置工作，自动识别并且修正系统漏洞的漏洞修补工具群集，随时观察主机进程活动和文件操作进程的情况发展，一旦察觉到有害进程或者可疑文件有变动迹象就立刻触发报警程序并采取隔离措施，由此构建起了“边缘阻挡，中间监督，节点守护”的完整技术链条，全面提升能源网络安全能力。

安全域划分技术：能源行业的业务形态多种多样，其数据的敏感程度也不尽相同，所以安全域划分技术按照业务的关键性以

及数据的敏感度等级，依靠资产的价值、威胁的概率和脆弱性的量化算法，并结合网络拓扑图绘制技术来准确地展现设备之间的互联情况以及数据的流向，从而达到灵活设置并动态调整安全域的目的，在此期间运用数据分类和级别划分的方法，在电力发电量、油气开采产量这些能源生产的数据上，还有客户的能源消费记录和个人的身份信息这样的隐私资料，实行标签化的分类标识，对各种类型的、不同层次的资料实施安全属性的标注；并且综合利用角色权限控制的措施，针对岗位上的员工执行权限分配的差异化处理，高级别的生产数据只能让能源调度人员查看，一般的行政职员只能阅读低级别的敏感办公资料，对于没有得到许可的人接触高安全区域内的资料要进行严格的检查审核，有效遏制了数据泄漏的源头，极大地提升了技术防御的准确性，去应对能源行业业务和数据安全方面复杂的需要。

（二）主动防护关键技术

智能防火墙技术：相较普通防火墙而言，智能防火墙技术把DPI 技术和行为分析技术结合起来，使得防护效果有质的变化，摆脱了传统防火墙只能按照预先设定好的规则来进行防护的局限性，深度包检测技术会对网络数据包的内容逐层开展内容挖掘工作，从而准确找出其中的数据包 IP 地址以及端口这些表面信息，可以深入挖掘数据包携带的应用层数据，剖析隐藏在 HTTP 协议数据包里的恶意代码，行为剖析技术运用机器学习这种技术手段来创建并分析网络连接活动，数据流动情况等，探究常规行为模型同现实网络行为之间存在的联系，以此来识别出异常的网络流量特性，就某个设备来说，如果短时间内不断出现异常链接的情况，并且其产生的数据流量远远大于正常的业务范围，即使攻击行为藏匿于合法的数据包之中也能够被察觉到。

IDPS 入侵检测防御技术前沿：采取特征对应，异常侦测以及机器学习算法的入侵检测防御技术，形成起多角度，精确度高的攻击检测体系，能源网络安全防护领域处于中心地位，依靠大量已知攻击特征的匹配算法，可以快速辨别常见的攻击举动，对于能源系统安全漏洞的 SQL 注入，缓冲区溢出之类的攻击途径，一旦察觉到攻击数据包同特征库存在匹配迹象，立刻激活防御措施；异常检测技术依靠创建能源网络正常运作的参照标准，当网络举动偏离预定轨道时，会马上触发警报机制，准确找出未知的以及新出现的变异攻击行为；该算法在能源网络的历史攻击记录和日常运行数据里不停地吸取知识，持续优化攻击识别方法，加强识别复杂攻击行为的能力。

数据加密核心技术：能源产业数据安全防护的实践与总结录，数据加密技术核心着力点在于存储和传送两个环节，形成起全方位的数据安全防护系统，在数据存储期间，重点放在能源企业的关键资料上，比如能源战略规划资料，核心生产技术资料以及客户隐私信息资料等，利用 AES，RSA 这些加密手段去加密数据，AES 加密技术因其强大的加密功能而知名，适合用于大量生产数据的加密存放，从而保证这些数据即使被存放在数据库或者存储服务器之类的介质当中也处于一种密文形式之中，若存储途径遭到窃取，由于没有相应的解密密钥，所以无法执行数据的读取操作，RSA 算法经常被用来守护加密密钥以及一些机密设置信息，它借助于公钥加密而私钥解密的方式提升了密钥管控的安全性。

（三）安全管理与应急响应技术

人员安全管理支撑技术：能源网络安全，人员因素处在关键地位，人员安全管理技术依靠线上线下的融合形式，达成技术上的辅助并加以改善，利用模拟攻击实战技术手段，全方位加强员工对于网络安全的认识以及防护技巧，这个在线教育平台集中了网络安全方面的教学影片，案例分析素材，在线测试题目等各类教学资料，岗位需求成为员工挑选职位的依据，了解网络安全的基本原理，而现场培训活动则通过请网络安全方面的专家做专题演讲，举办现场实操教学之类的活动来开展，针对能源行业普遍存在的一些安全隐患展开剖析，包含钓鱼邮件袭击，随意使用移动储存装置等等情况，从而让员工认识到这些安全隐患并学会应对之法。

应急响应技术：即时回应能源产业网络安全威胁，应急处理技术包含安全监控平台、日志剖析以及自动化应急体系，创建起精妙的安全事件应急模式，有效解决安全问题，安全监控平台(SOC) 处于中心地位无法撼动，及时整合能源网络内各种设备（比如路由器，交换机），服务器（生产调度服务器，数据库服务器）以及终端设备（员工办公电脑，生产现场终端）的运作情况和安全事件消息，图形化界面清楚显示网络安全状况，方便安全管理员随时掌握网络动态；大数据算法带动日志剖析深入探究，针对收集起来的大量日志材料（设备登录信息，数据传送信息，系统操作信息等）展开深度剖析和挖掘，从繁杂的日志信息当中找出不合常理之处，某台服务器在非工作时段经常创建外部链接，核心数据库向外部 IP 地址短时间内传输大量数据这些情形，迅速察觉潜在危险迹象。

四、结论

网络安全关键技术属于能源行业数字化转型安全进程中的坚固支撑，面对繁杂的安全问题，能源公司要加大分层防护，积极防御以及数据加密这些关键技术研发并加以运用执行力度，塑造起一种“技术改良 -- 运作简化”的循环结构体系，依靠技术改进与操作成果转换来提升网络安全防护的准确度及其实效，从而保障能源生产和运作的稳定与安全状况，新的技术更迭波浪接踵而至，能源网络安全技术架构持续更新换代，创建起国家能源安全方面的科技屏障。

参考文献

[1] 杜敏 . 加快推动能源产业与数字技术融合发展 [N]. 中国电力报 ,2024-10-28(005). DOI:10.28061/n.cnki.ncdlb.2024.002332.

[2] 曾小明，李伟，张全东，等 . 防火墙技术在能源行业网络安全保障中的应用 [J]. 网络安全技术与应用 ,2024,(06):128-130.

[3] 王英梅，王连庆，杨林，等 . 能源行业多维协同驱动下的网络安全教育体系创新与实践 [J]. 中国信息安全 ,2025,(04):33-36.

[4] 曾小明，李伟，张全东，等 . 防火墙技术在能源行业网络安全保障中的应用 [J]. 网络安全技术与应用 ,2024,(06):128-130.

