面向四川电力业务运行的信息安全保障体系构建研究

杨嘉湜,杨 帆
(国网四川省电力公司信息通信公司,四川 成都 610041)

摘 要:随着国网四川省电力公司信息化建设工作的深入,以及大量新技术在电力信息行业的广泛应用,信息安全,特别是设备、网络和数据安全面临着越发严峻的挑战。如何通过行之有效的手段保障公司信息运行安全,是电力信息行业面临的关键问题。从日常运维工作实际出发,以安全保障需求为基础,结合业界单点式安全防御手段的应用,率先将管理和技术两方面视为一个有机整体,通过对每一方面的关键要素进行分析,构建了面向电力行业信息安全的保障体系。事实证明,该体系对消除信息安全保障死角、提升信息安全水平、提升IT保障能力和数据安全能力有重要的指导意义。

关键词:防御体系;网络攻击;业务审计;数据脱敏;安全责任
中图分类号:TM761 文献标志码:A 文章编号:1003-6954(2018)03-0088-04
DOI:10.16527/j.cnki.cn51-1315/tm.2018.03.018

Research on Construction of Information Security System for Sichuan Electric Power Service

Yang Jiashi, Yang Fan
(State Grid Sichuan Information & Telecommunication Company, Chengdu 610041, Sichuan, China)

Abstract: With the construction of information system and the application of a large number of new technologies, the information safety, especially the equipment, network and data security face severe challenges. In this case, how to ensure the security of system operation by some kinds of effective methods needs to be considered. Starting from the daily practical operation and based on security requirements, the technology and management are considered as an organic whole. Then the key elements in each aspect are analyzed, and the information security system for electric power industry is constructed. It has been proved that the system can effectively improves the ability of information and data security.

Key words: defense system; network attack; operational auditing; data masking; safety responsibility

0 引 言

随着国网四川省电力公司(以下简称四川公司)信息通信系统与电网安全生产、日常经营活动深度融合,信息专业已成为大电网运行控制和四川公司生产经营管理的重要基础。与之对应的是,该专业具有数据量大、分布面广、利用价值高、技术复杂度高、运行渠道多样化等特点[1],给工作带来便利的同时,各类外部攻击和数据泄漏风险大幅提升。国网四川省电力公司信息通信公司(以下简称信通公司)作为四川公司信息化支撑单位,运行维护着全省绝大多数信息系统和通信信息骨干网络,肩负着重要的政治责任、经济责任和社会责任。全新的形势带来了全新的要求,信通公司平台安全防护面临着严峻挑战。

1 问题分析

当前,四川公司面临的信息安全形势空前严峻。电网生产运行高度依赖网络和信息化,一旦外部攻击突破安全防护体系,将直接威胁电力系统安全[2]。信通公司支撑着四川公司各业务部门生产、营销、财务、人资、ERP、电力交易等逾百套信息系统的运维工作,管理着超过数百T的核心数据,服务着超过10万内部用户和数千万外部电力用户,存在大量可能具有安全隐患的环节,信息安全如履薄冰。

1)网络攻击威胁日益增加。网络攻击技术与

(C)1994-2021 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

手段的迅速发展，网络安全攻击的针对性、持续性、隐蔽性显著增强，大大增加了网络安全防护难度，甚至造成严重的损失。2017年迄今为止，信通公司监测并拦截互联网出口高风险攻击数量295.96万余次，比去年同比增加11.58%；外网网站遭受攻击数量2 543.2万余次，比去年同比增加12.48%。

2) 信息安全运行压力大。随着信息通信系统规模和应用范围的大幅持续增长，信息通信系统大面积停运的风险不断增加，尤其是因信息通信故障导致大面积停电的风险依然存在。

3) 信息安全边界持续扩大。四川公司信息化应用由内网为主、向内外网协同转变，接入方式由有线向无线演变，全业务统一数据中心、移动作业终端、光伏电厂、风电厂、充电桩、计量采集终端、智能电表等新业务的安全管理存在隐患，安全防控难度陡增[3]。

4) 服务对象范围不断膨胀。四川公司的公众服务业务作为面向用户的服务窗口和展示形象，存储了大量公众客户的敏感信息，智能电表和掌上电力等营销类自动缴费业务应用的推广，在带来业务创新的同时，也引入了工控安全风险，随之而来的还有权限、内容、数据、操作等各类安全风险不断扩大[4]。

由此，怎样坚决贯彻落实国家电网公司战略部署，做好信息安全工作，保障信息通信专业的稳定、可靠运行和服务，构建符合电力行业特点的信息安全保障体系，是信通公司一项重大课题，也是推动公司面向电力市场竞争新形势发展的必然要求。

2 信息安全保障体系构建

2.1 总体架构

信息系统现阶段自动化和智能化程度有限，其稳定运行的核心因素依然是各级从业人员及其在运维过程中的操作，构建适应四川公司实际工作特点的信息安全保障体系至关重要。显然，仅依靠技术手段规范人的行为，很多时候会失之于僵化；而仅依靠管理手段则常常失之于松软。因此，“人防”与“技防”双管齐下，从两个方面同步规范运维人员日常工作，才能达到期望的效果。信息安全保障体系的基础架构如图1所示。

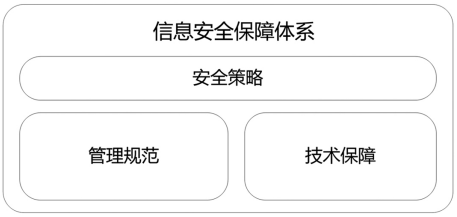

图1 信息安全保障体系基础架构

信息安全保障体系设计的初衷，是从技术和管理两个层面保障四川公司信息系统、网络及数据的运维安全，达到底层支撑服务保密、完整、可用等安全目标。其中，技术体系重点关注系统的安全防护、检测、响应和恢复，而管理体系则着重强调日常工作的合规性和人员管理的严密性，通过完善的管理流程和制度标准对运维过程进行规范，在统一的安全策略指引下，共同保障信息安全保障体系的有效性。

2.2 管理要素

管理体系是信息安全保障体系的总体原则，也是保障体系落地的制度保障。因此，管理体系应当从四川公司的整体出发，全面考虑各方面安全管理问题，健全四川公司信息安全管理组织和管理机制，结合完善的安全管理制度，覆盖公司信息安全的全流程，其要素如表1所示。

表1 管理体系基本要素

基本要求	项目描述
安全管理制度	信息安全制度完善
人员安全管理	人员安全能力建设
系统建设管理	第三方运维管理
安全责任	逐级落实运行安全责任
风险评估	风险评估能力建设
日常维护	配置管理规范建设 网络安全流程规范完善

1) 落实安全责任

全面开展《网络安全法》[5]宣贯培训，做到深入理解、逐条落实，将网络安全法要求制度化，牢固树立风险意识，充分认识责任义务，层层签订安全责任书，将相关责任压紧压实，直至贯穿公司全业务、全环节、全过程。

2) 完善安全制度

以标准化为目标，通用制度为准绳，构建四川公司标准化制度体系。利用信息专业独特优势，构建管理统一、职责明确、界面清晰的四川公司信息安全管理体系、监督体系和保障体系，发挥信通公司在信

(C)1994-2021 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

息化建设与业务部门支撑中承上启下的作用，强化内控机制[6]，坚持内控与外防并重、人防与技防并重，对各类违规、违章和网络信息安全事件，严肃问责、坚决处理。借鉴营销、财务等专业的标准化服务体系，明确各专业信息安全管理体系关键节点和要素，打造标准化制度体系，力争实现信息通信运维服务从“面向设备”到“面向业务”，从“支撑业务”到“推动业务”，最终到“面向服务”的转变。

3) 提升履职能力

人才是发展的第一资源。严格贯彻落实四川公司安全工作要求，加强与各业务部门的沟通，结合表1梳理的信息安全管理体系关键节点所必需的要素，常态化开展相关培训，做到梳理一项，培训一项，落实一项，创新人才培养体制机制，提升信息安全履职能力。

4) 系统建设管控

建立第三方安全管理的规范和制度，并要求其严格遵守。严格控制第三方对信息系统的访问，对第三方访问的风险、人员及运维管理进行风险评估，并在合同中规定其安全责任和安全控制要求，以维护第三方访问的安全性。

2.3 技术要素

信息安全技术是信息安全保障体系构建的底层保障，也是管理层面的具体落脚点，对保障体系构建尤为重要。信息安全的技术实现应当遵循先进性、实用性、可靠性及可扩展性原则，既能够应对信息系统运维现状，又能以足够的能力满足四川公司未来业务发展的需求，其架构如表2所示。

表2 技术体系基本要素

基本要求	项目描述
网络安全管理	网络安全域划分及改造
业务安全管理	业务安全审计及态势感知
漏洞管理	漏洞扫描
数据库安全管理	数据库防护
文档安全管理	电子文档安全审计
终端安全管理	对网络终端的主动管理分发
数据安全管理	数据脱敏

1) 网络安全域划分及改造

通过安全域划分及改造，能够从网络基础层面实现对外部攻击进行层次化、立体化防御，从而进一步落实安全管理政策、制定合理安全管理制度的基础。

2) 业务安全审计及安全态势感知

业务安全审计通过网络对各服务器系统、数据的访问行为进行审计和控制，使运维操作符合企业合规性的需求，并做到操作的可审计、可追溯，能够建立有效的IT内控机制，提升业务操作的可靠性，减少核心数据资产的破坏和泄漏。同时，安全态势感知则通过对流量和安全事件的采集和分析，有助于更加直观地掌握业务系统运行的安全状况。

3) 漏洞扫描

漏洞扫描能够在对网络设备、操作系统、应用系统的扫描过程中有效发现系统弱点，为实施安全防护方案和制定安全管理策略提供依据和参考。

4) 数据库防护

数据库防护通常通过数据库防火墙实现，具备屏蔽直接访问数据库的通道、对应用程序访问数据库进行二次认证、对数据库进行攻击保护、连接监控、安全审计等能力，能够有效提升数据库安全防护水平。

5) 电子文档安全审计

电子文档安全审计能力通过具备电子文档安全保障能力的系统实现。其能在服务器上备份所有的文件审查日志，根据用户角色不同，将用户权限精准划分和分配，能够让用户在无感知的前提下极大提升数据的完整性和可靠性。

6) 终端安全管理

终端安全管理能够实现对网络终端进行主动的管理和控制、补丁分发、强制安全策略、远程帮助等主要功能，并形成整体的安全准入控制体系，其提供网络准入控制、应用准入控制、客户端准入控制等多层准入控制手段，实现对终端安全接入内网管理。通过准入控制机制，可以实现对终端的身份进行认证，并能够自动检测和修复终端安全状态，强制保证终端及时进行安全补丁更新、安装并及时更新防病毒软件及病毒定义码、不随意运行可能存在风险的软件，确保只有合法的和安全的终端电脑才能接入企业内网。同时，利用生物特征识别技术，强化操作人员个人身份的确认和权限的认定，克服传统账号及密码登录方式的繁琐和隐患，提升终端安全管理水平。

7) 数据脱敏

数据脱敏能够根据不同需求隐去涉密内容，保留数据业务含义的基础上隔绝系统开发或未经授权的用户接触核心真实数据的路径[7]，同时通过在线或离线脱敏规则，在保障业务研发进度的基础上，降

(C)1994-2021 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

低数据运维工作量及难度，最大程度地规避数据安全风险。

3 结 语

随着信息化建设的持续深入，大数据、云计算、区块链等新技术的逐步应用，以及业务需求的持续增长，安全一直是信息运维永恒的话题。从信息安全保障的实际需求出发，构建了信息安全保障体系，并分别从管理和技术两个层面阐述了其架构和包含的关键要素。安全管理持续推进的事实证明，该体系能够有效地消除信息安全管理死角，夯实信息安全基础，提升信息系统安全保障水平，切实承担起智能电网和“五大”体系高效运转的支撑职责，为四川公司筑起一道安全的“防火墙”。

参考文献

[1] 李文娟，胡珺珺，赵瑞玉. 通信与信息专业概论[M]. 北京：人民邮电出版社，2014.
[2] 曾鸣，李娜，董军，等. 基于大安全观的电网运行管理关键技术——关于印度大停电的思考[J]. 电力系统自动化，2012，36(16)：9－13.
[3] 贺惠民，王刚，陈乐然，等. 智能电网信息安全问题与优化研究[C]. 中国电机工程学会年会，2013.
[4] 周文琼. 大数据环境下的电力客户服务数据分析系统[J]. 计算机系统应用，2015，24(4)：51－57.
[5] 孙昌军，郑远民，易志斌. 网络安全法[M]. 长沙：湖南大学出版社，2002.
[6] 王凡林，陈辉，王寿荣. IT治理机制下的企业内部控制问题与建议[J]. 会计之友，2011(3)：70－71.
[7] 姜日敏. 电信运营商数据脱敏系统建设方案探讨[J]. 中国科技信息，2014(8)：132－133.

作者简介：

杨嘉湜(1963)，硕士研究生、高级工程师，从事电力系统自动化及电力通信信息专业工作。

(收稿日期：2018－05－04)

(上接第60页)

预测模型，如BP神经网络方法、专家系统法和支持向量机(support vector machine，SVM)法[14]，这些方法可以有效地计及影响电力负荷的诸多外在因素，从而训练出精度较高的预测模型。在中长期电力负荷预测时，可以运用回归分析法、趋势分析、电力弹性系数、产值单耗等方法，通过大量历史数据或经济指标数据支持，对平稳且大量的数据有不错的预测效果。四川省未来电力负荷预测应采用以智能化和传统方法相结合的新型预测方法，如空间负荷预测(SLF)元胞分析模型、改进型灰色模型等组合算法，这将更适应不断暴露出来的负荷曲线波动问题。新型负荷预测问题的不断出现也将带动电力负荷预测技术向更深层次发展，而电力负荷预测也将为中国建成“一带一路”经济强国、全球电力市场互联互通提供坚强护盾与有力支撑。

参考文献

[1] 张彦宇，肖茜. 国内外关于电力系统负荷预测的研究现状分析[J]. 山东工业技术，2016(11)：215－216.
[2] 刘建军. 电力系统负荷预测综述[J]. 中国科技信息，2016(16)：52－53.
[3] 于杏. 电力负荷预测方法分析[D]. 南京：南京理工大学，2016.
[4] 宋晓茹，李莉，张来青. 中长期电力负荷预测研究[J]. 计算机仿真，2014，31(9)：132－135.
[5] 罗国东. 基于改进电力弹性系数法的负荷预测[J]. 陕西电力，2013，41(6)：46－48.
[6] 李钜，李敏，刘涤尘. 基于改进回归法的电力负荷预测[J]. 电网技术，2006，30(1)：99－104.
[7] 杜莉，张建军. 神经网络在电力负荷预测中的应用研究[J]. 计算机仿真，2011，28(10)：297－300.
[8] 朱建平. 神经网络在电力负荷预测中的应用研究[J]. 科技资讯，2015(23)：32－34.
[9] Willis H L. Spatial Electric Load Forecasting[M]. New Work: Marcel Dekker，2002.
[10] 肖白，杨欣桐，田莉，等. 计及元胞发展程度的空间负荷预测方法[J]. 电力系统自动化，2018，42(1)：61－67.
[11] 俞明生，冯桂宏，杨祥. 组合优化灰色模型在中长期电力负荷预测中的应用[J]. 沈阳工业大学学报，2007，29(2)：153－156.
[12] 肖白，周潮，穆钢. 空间电力负荷预测方法综述与展望[J]. 中国电机工程学报，2013，33(25)：78－88.

作者简介：

杨博宇(1990)，博士研究生，研究方向为水电运行管理及电力市场；

陈仕军(1989)，博士、助理研究员，研究方向为水电运行管理与电力市场、能源战略与经济管理。

(收稿日期：2018－03－06)

(C)1994-2021 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net