浅析电力行业大数据应用及安全风险

  作者：中国信息安全测评中心 宋璟 任望 王煜 佟鑫   时间：2017-11-01

   随着信息化建设的推进，电力行业在日常生产、经营和管理中会产生大规模、多种类的数据信息，传统的数据处理机制面临处理庞大规模数据乏力、时效性差，对诸如图片视频等数据处理能力明显不足的窘境。大数据技术在电网中的应用，依靠集群力量对数据进行分析处理，支持半结构化和非机构化数据的处理能力，突破了传统技术的瓶颈，带来了巨大的技术变革，同时在优化电力企业管理、提高企业价值、创新电力业务模式等方面，都发挥了巨大作用。

**电力行业大数据的价值应用**

**1. 基于大数据的用户能源分析及用电方案优化**

   随着智能电网、用电信息采集系统的建设和应用，智能电表每日产生大量、不同类型的用电相关数据，以省为单位的用户用电数据可以达到几千万条，利用这些数据结合气象数据、用电信息、电费信息、企业生产数据及用户负荷等数据的价值，采用分布式计算、数据挖掘等技术，研究用户的负荷特性及用电行为习惯，构建用户用电意愿、业扩报装、环境因素、行业用电结构变化与电量变化影响关系的知识库和关系模型，可以对用户用电能耗进行分析和信息推送，最终引导用户合理优化用电行为。基于大数据的用户能耗分析及用电方案优化可以提高能源利用率，降低用能费用，保障客户经济利益的同时，也有利于电网削峰填谷，平稳运行，提升供电服务满意度。

**2. 通过电力大数据开展物资管理**

   物资管理是电网运行必不可少的环节，在物资管理中需要对公司物资库存影响进行分析。通过分析当年项目投资的规模，定性的估算物资库存需求，安排相应的物资采购计划，并将物资采购数据录入公司的ERP、电子商务平台，生产管理系统、营销业务系统中，利用大数据关联分析技术，开展物资库存、物料需求与电网规模、结构、年限以及投资等信息的关联分析，研究其存在规律，获取合理的安全库存预估方法。最终实现仓储陈本最小化，提高库存合理性和资金使用率。

**3. 利用大数据开放、共享的特性促进业务融合**

   电网中长期负荷预测是电力调度部门制定电源、电网规划方案的基本依据，其数据源涵盖气候、历史用电量、政策等方面，这些数据分别存放在不同的机构部门中。利用分布式存储和数据采集技术，将这些分散的数据集中采集处理。而后通过数据挖掘技术，根据用电信息采集数据、行业用电信息和产能信息等数据，统计分析行业的负荷用电信息，获取行业用电特征和单位规模用电量。结合政府用地规划数据和原有地理信息数据，预测地区用电负荷。通过将价值数据共享，一方面有利于中长期负荷预测数据查找的工作冗余，另一方面也为其他部门制定规划方案、政策提供了参考依据。

**电力行业大数据面临的安全风险**

   随着全球能源互联网重要战略的实施，“互联网+”智慧能源的快速发展，智能电网（尤其是微网、智能配电网、智能电表）的全面建设，使电力行业大数据地理分布面更广、数据采集点更多、数据类型更多、业务关联关系更复杂,数据的使用方式和使用者更加广泛，那么在给电力生产、营销带来便利的同时，也给电网大数据安全带来以下风险：

**1. 电力行业大数据存在数据泄露风险**

   电力在其整个“发、输、变、调、配、用”的周期中，每个环节、每个瞬间都在产生海量的数据，如在电网运行过程中通过各类传感器实时或定期获取设备状态信息，仅涵盖主网设备的情况数量级可以达到TB级。配网设备数据量更大，种类繁多，随着配网设备逐步集成到设备生产管理系统，数据规模将达到PB级；在营销客服领域目前仅用电信息采集一项，每年新增数据约90TB，客户服务数据全年预增7TB。这些数据均可极大促进电网智能感知、内部管控能力以及用户服务效率提升，但如果数据提供者对数据的采集、传输、存储、处理、使用过程中无法实施有效的控制，那么可能造成海量敏感数据泄露。例如，有些收集数据的本地收集终端还留存有数据，缺乏对留存数据的安全保护机制；本地智能终端与后台服务器之间缺乏数据传输安全机制，采集系统缺乏身份验证、权限管理、加密、完整性校验等安全机制等等都会造成数据破坏或泄露。一旦大数据被篡改、泄露，将会对电网生产、经营管理、用户服务造成极大的影响。

**2. 电力行业大数据更易成为网络攻击目标**

   电力作为各国家关键基础设施，一旦发生网络战争必然成为网络攻击的首选目标，例如“乌克兰停电事件”还是“震网病毒”攻击伊朗核设施事件。那么，电力大数据好比是一座“金矿”，有人想从中“淘金”，有人想往其中灌“沙子”，这使大数据成为一个可利用又可攻击的载体，一些黑客将恶意软件和病毒代码隐藏其中，达到攻击并篡改、窃取数据目的，最典型的就是APT攻击。通过攻击获取电力大数据价值信息，可以分析出攻击目标所在地的用电分布、关键信息基础设施的位置，篡改关键节点监测预警信息、操作指令等关键数据，造成电力系统故障或重大安全事故。同时，电网是公用事业企业，服务于社会大众，如涉及客户的大数据保护不当被攻击，如用户电量、电话号码、家庭地址等敏感信息被泄露，均会对社会公众安全产生负面影响。

**3. 电力行业大数据安全管理是最突出的风险**

   数据安全管理问题，是我国应用大数据面临的最突出风险。虽然将海量数据集中存储，方便了数据分析和处理，但由于安全管理不当所造成的大数据丢失和损坏，则将引发毁灭性的灾难。由于新技术和新业务发展，对隐私权的侵犯已经不再需要物理的、强制性的侵入，而是通过各类数据更加微妙的方式广泛衍生，由此所引发的数据风险和隐私风险，也将更为严重。2016年，某电网在推行网上增值业务的时候，第三方服务公司通过地方供电所提供的信息，开展业务代办服务，间接实现了信息收集，导致大规模数据泄露事件发生。而数据安全管理机制和信息监管的缺乏，导致数据所有者无法明确在信息记录的后台，有谁记录了信息，下载了数据，使从收集到生产、分析、发布等各个环节都没有数据隐私保护，电网用户的信息安全受到了极大的危害。

**电力行业大数据安全防护建议**

**1. 做好电力大数据全生命周期的安全保护**

   电力大数据来自于生产数据和运营管理数据，应针对其防护应重点从数据采集与传输、存储、使用等数据全生命周期开展安全保护工作。从数据采集到数据传输的加密保护，数据存储的可用性完整性保证，再到数据使用和恢复的准确性要求，期间应从政策制度要求到技术管控，全面评估关键数据所面临的威胁暴露面，有针对性地制定各阶段防护策略，确保核心数据资产安全。转移数据防护重心，由“基础防护”向“精准防护”合理转变，解决价值数据安全“看不见、看不准、看不实”的问题。

**2. 提升电力行业大数据安全管理能力**

   “数据安全三分靠技术，七分靠管理”。电力海量数据中不仅包括大量用户隐私信息，还涉及企业经营决策信息，甚至关系国计民生以及国家决策的重要信息。以用户隐私为例，如目前第三方交互支付平台缴电费过程中，对一些用户地址、联系方式等隐私信息进行部分隐藏式的显示，以避免信息泄露，同时隐私信息不提供第三方存储。在开展电力大数据的安全管理方面， 一是做好电力大数据建设的规范统一。制订电力行业统一的安全规范框架，各级各类信息的网络互联、数据集成、资源共享、全周期隐私保护均在统一的标准下运行，实现大数据管理和使用的正规有序。二是做好电力大数据安全风险评估。针对电力大数据的不同类别，如营销数据、用电数据、预警数据等按照重要程度分类管理，设置不同的安全风险等级，制订安全防范措施，最大限度降低用户用电信息泄露的隐患。三是要提高电力企业员工安全意识。对企业存储的电力大数据类型和数据防护知识开展培训，让员工意识到数据的价值，充分认识自己工作中数据安全的重要性。结合实际周期性地进行安全攻击演练，提高防范效果。

**3. 加强电力行业基于安全大数据的技术防护**

   所谓的安全大数据是指业务安全、系统安全、网络安全、硬件安全有关的配置数据、实时数据、衍生数据等。我们的目标是通过有效的数据挖掘算法从各类数据中发现隐含的有意义的信息从而为安全提供支撑和保障。电力行业应建立基于安全大数据的威胁发现技术，超越以往的（P2DR）模式，更主动地发现潜在的安全威胁，例如某电网正在试运行的安全SOC平台（S6000）。通过在威胁检测方面引入大数据分析技术，可以更全面地发现针对企业数据资产、软件资产、实物资产、人员资产、服务资产和其它为业务提供支持的无形资产等各种信息资产的攻击。通过建立基于安全大数据分析技术，可以使分析内容的范围更大，威胁分析窗口可以横跨若干年的数据，因此威胁发现能力更强，可以有效应对APT类攻击。

**4. 用战略和长效的眼光思考安全问题**

   大数据对电力行业带来了机遇也带来了挑战，大数据在电力行业应用越广泛，其带来的价值也越大。以数据安全为中心的安全管理理念将改变传统的工作思路，必须要从大数据安全战略角度来认识电力信息安全问题，必须要认清国内外大数据安全的新变化、新特点、新趋势，深入分析当前形势下的大数据安全的突出问题，明确我国大数据发展的战略目标和战略重点，统筹谋划电力大数据应用、关键技术研发、数据保护、法律法规等关键布局，才能确保我电力大数据信息安全发展战略与我国国情保持一致，并不断完善。

**5. 正确处理电力大数据发展与安全的关系**

   正确处理发展与安全的关系，“以安全保发展，在发展中求安全”，保障安全、促进发展是贯穿科学建立电力大数据安全技术体系，促进电力大数据发展的根本原则。从以往信息安全的发展成熟度来看，大数据安全保障的应用效果也不会立竿见影。应发展自主可控的电力大数据技术与加强信息安全管理并重，加快建设信息安全基础设施，发展大数据安全产业，改善基础应用环境，做到“基础安全有保障”，在这个前提下，以风险评估、等级保护等多种手段为依托，承受一定范围的可控风险，全速发展电力大数据安全工作。

**结语**

   数据即资产，电力大数据是电力企业的重要资产。电力大数据技术的成熟将驱动电力公司对数据由定性分析向定量分析转变，促进业务管理向着更精细、更协同、更高效的方向发展。后期以大数据为核心的泛在智能电网，将优化能源的生产方式、利用方式以及消费方式，如清洁能源、电动汽车的发展和利用等，有望催生新的经济模式。从这个层面看，在构建全球能源互联网的进程中大数据必将发挥越来越重要的作用。

   需要注意的是，虽然各电力企业的信息化建设已经初具规模，但电力大数据目前仍处于前期研究阶段，电力大数据面临的风险和安全问题还比较突出，当网络中传输的不仅仅是电能，更重要的还有数据，这就需要电力企业、安全厂商、国家网络安全权威机构通力协作，更积极主动探索如何确保电力大数据的网络安全，如何开展电力大数据安全保障，如何从顶层设计、管理体系和技术防护等角度强化大数据的安全与保护，只有这样才能够真正地推动传统电力工业的升级，为“建设全球能源互联网、建设安全高效的现代能源体系”保驾护航。