内外网数据安全交换技术在电网企业的应用研究

郭仁超[1],徐玉韬[2]
(1. 贵州电网有限公司信息中心,贵州 贵阳 550002;
2. 贵州电网有限公司电力科学研究院,贵州 贵阳 550002)

摘 要:为保护企业机密,需要采用安全有效且成熟的技术来保障企业信息安全。以网闸等安全设备为基础的内外网数据安全交换平台,通过网络隔离、安全访问控制、协议剥离重组等技术,实现可控安全的数据交换,建立一套完善的内外网数据安全交换系统。本文参考电网企业安全防护标准、公安信息通信网边界接入平台安全规范及其他行业内外网安全防护设计思路,结合电网企业的应用需求,提出了多层次安全隔离防护,强管控数据交换的安全策略,并设计了符合电网企业应用需求的内外网数据安全交换平台、数据交换体系和安全管控方法,实现了电网企业内外网安全数据交换。同时结合试点、推广建设与实践,阐述了该体系在电网企业内外网实际环境中的应用效果。

关键词:网络隔离;信息交换;访问控制;安全管理
文章编号:2096-4633(2018)02-0061-06 **中图分类号**:TM63 **文献标志码**:B

现代社会对电力供应的可靠性要求越来越高,电力安全工业的地位比以往任何时候都更加重要。随着“互联网能源”以及“能源互联网”的发展,过去在管理信息大区与互联网之间、信息大区内部之间采用单一、同构的防火墙技术保护内外网边界,实现电力二次系统安全防护的安全措施已无法应对互联网新型网络攻击的威胁,也无法满足互联网复杂应用场景下的安全防护要求[1]。

1 新型互联网攻击威胁

随着互联网攻击技术的发展,APT(高级持续性威胁)/AET(高级逃逸技术)、蠕虫、网页挂马等新型网络攻击形态层出不穷,这类威胁具有高度的隐蔽性,甚至会透过梯次渐进的方式,穿透电力监控系统横向隔离、纵向认证等安全防护机制,威胁到生产控制大区和电力调度数据网,从而对电力安全生产产生重大影响[2]。2011 年著名的伊朗核电站遭受“震网”蠕虫病毒攻击就是典型的 APT 攻击案例。2015 年 12 月 23 日,乌克兰伊万诺弗兰科夫斯克等三个区域电力系统被具有高度破坏性的 BlackEnergy 恶意软件攻击并导致大规模的停电,成百上千用户居民家中停电,城市陷入恐慌当中损失惨重。此时事件是典型的黑客组织利用技术制造的 APT 攻击事件。BlackEnergy 恶意软件新增的 Killdisk 组件专门破坏工控系统(ICS)或者 ELTIMA 系列以太网连接器,并可以设置后门从而远程控制关闭电力控制系统。

2 互联网复杂应用场景下的安全防护要求[3]

电力系统过去相对封闭的管理信息区应用系统在互联网应用场景下,需要进一步开放服务,更紧密地与用电企业、家庭、互联网第三方服务机构以及电力办公、营销、检修人员结合,并通过互联网提供更高效、便捷的电力服务,这些服务不仅仅停留在简单的网站信息发布层面,还存在大量的移动互联和双向交互,包括通过大量的业务应用服务接口、网络服务以及数据库服务实现内外网间复杂的多类型信息交互,这些信息交互的安全性需要得到全面保护。

综上所述,电网企业应增强对管理信息大区外部网络边界的安全防护等级,采用防御功能更完善、安全防护能力更强的内外网数据安全交换技术[4]。

面对互联网下复杂的安全环境,电网企业应加强互联网出入口的安全防控能力,建立多层次防护、逻辑强隔离的内外网数据安全交换平台,为电力企业信息系统提供综合性的安全服务保障,有效抵御互联网攻击威胁,主要需求如下:

(1)加强内外网数据流向的访问控制措施,保障内外网数据交换安全;

(2)满足应用系统对内外网隔离环境下各种类型业务数据交换的需求;

(3)强化通信协议和信息内容控制能力,确保数据交换过程协议的安全可控;

(4)强化内外网应用交换对象控制,确保只允许合法应用和数据进行交换;

(5)落实数据安全监控管理,对数据交换过程进行实时监控。

本文针对电网企业互联网应用安全威胁,结合内外网数据交换应用需求,对内外网数据安全交换技术进行研究,提出了多层次隔离防护,强管控数据交换的安全策略,并设计了符合电网企业应用需求的内外网安全交换平台、数据交换体系和安全管控方法,对实际应用成效进行了分析研究。

3 内外网数据安全交换技术

3.1 内外网数据安全交换技术设计思路

电网企业内外网安全防护平台总体设计思路是在《电力行业信息系统安全等级保护基本要求》、《电力监控系统安全防护规定》(国家发展和改革委员会令 2014 第 14 号)以及配套的《电力监控系统安全防护总体方案》的基础上,借鉴其他行业内外网安全交换技术标准与最佳实践,结合电网企业的实际情况与互联网应用需求,全面梳理电网企业互联网应用系统业务功能和信息流,建立完善的内外网数据安全交换体系[5],主要思路包括:

(1)建立多级隔离,逐级增强的安全架构。以网络隔离与信息摆渡为核心,向内外网扩展安全防御层次,构建三级防护体系,从 WEB 应用、数据库和内外网隔离与信息摆渡等多个安全维度全面防护信息流途径的关键节点,全面封堵互联网攻击路径,适应电网企业互联网场景下对 WEB 漏洞、数据库、APT/AET、蠕虫等多类型互联网攻击的安全防护技术要求。

(2)建立丰富的数据交换体系,提供灵活、多样的数据交换方式,满足电网企业各类应用系统对内外网数据交换的需求。

(3)建立内外网应用系统间安全的状态信息交互机制,保证应用系统数据交换的完整性、可靠性[6]。

(4)建立严格的人员与设备安全准入机制和数据交换控制机制,制订以安全接入控制、文件级数据交换和内容深度过滤为基石的信息摆渡安全策略,严格控制内外网数据交换行为、格式内容和方向,保证内外网数据交换的安全性。

(5)建立高性能、高可用性的交换体系,提供应用级负载均衡、双机热备等功能,保障内外网数据安全交换体系的鲁棒性和交换性能[7]。

(6)建立集中安全管理系统,实现内外网边界统一安全管理与应急响应。

3.2 内外网数据安全交换技术整体技术框架

电网企业内外网安全防护平台划分为四个安全域,建立三级防护体系。四个安全域分别为:

信息外网接入区。连接互联网的网络及路由设备区域,负责实现互联网的接入。

信息外网业务区。应用系统部署在外网的前置应用服务器区域,包括 WEB 服务器等,负责对互联网用户提供电力信息 WEB 门户服务。

信息外网数据区。电力应用系统部署在外网的前置数据库服务器区域,包括数据库服务器等,负责对 WEB 服务器提供数据库服务。

信息内网数据区。应用系统部署在内网的主系统数据库。

3.2.1 “多层次、强管控”安全防护平台设计

三级防护体系建立了多层次的防护体系,同时,通过加强对关键性、安全薄弱节点的重点防护,加强内外网数据安全交换的管控力度对保证电力信息内网安全十分重要。本文针对电网企业的应用情况,并参考其他行业内外网安全交换平台的优缺点,重点设计了实现二、三级防护的内外网安全交换平台,加强数据库防护、内外网数据交换和安全管理的管控力度[8]。

内外网数据平台由数据库隔离装置、安全隔离交换装置和平台集中管理系统构成,其中,安全隔离交换装置由数据安全交换组件(外网)、安全隔离组件、数据安全交换组件(内网)、边界防护组件四大组件构成。

数据库隔离装置用于抵御来自信息外网的违规或恶意数据库操作行为,保护部署在信息外网上的应用系统数据库安全,实现数据库访问控制、数据库访问进程校验、数据库重点库表防护、数据库高危操作过滤、数据库入侵阻断以及数据库操作审计等安全功能[9]。

安全隔离交换装置用于信息内、外网间的逻辑

强隔离与信息摆渡交换,在断开信息内网与信息外网网络连接的前提下,实现对信息内、外网数据交换的身份认证、访问控制、内容过滤、格式检查、病毒查杀、安全缓存、数据抽取/转换、交换操作审计等安全功能。安全隔离交换装置由数据安全交换组件(外网)、安全隔离组件、数据安全交换组件(内网)、边界防护组件等组件构成[10]。

数据安全交换组件由内、外网数据安全交换组件构成,用于实现信息内、外网数据安全缓存与交换,防止对信息内网的非法访问和信息泄漏,并实现内容过滤、格式检查、病毒查杀、应用级安全认证等安全功能。数据安全交换组件的功能主要由数据落地缓存、结构化数据安全交换、非结构化数据安全交换、混合类型定制化数据安全交换、应用代理高强度安全交换和消息服务等逻辑组件实现。各组件的主要功能如下:

数据落地缓存:用于实现信息内、外网应用系统与内外网数据安全交换平台之间数据交换过程中数据落地缓存的功能单元。数据落地缓存为应用系统提供结构化和非结构化数据读、写缓存服务,是信息外网业务区和数据区与信息内网数据区应用系统之间进行数据交换的中间介质,保证内外网隔离环境下进行裸数据交换。

结构化数据安全交换:用于实现结构化数据交换的功能单元,提供数据库表单等结构化数据交换、数据内容检查、病毒过滤、格式转换、数据完整性验证等功能。

非结构化数据安全交换:用于实现非结构化数据交换的功能单元,提供文件、图片、HTML、音视频等非结构化数据交换、数据内容检查、病毒过滤、格式转换、数据完整性验证等功能。

混合类型定制化数据安全交换:用于实现混合类型定制化数据安全交换服务的功能单元,提供短信息、结构化数据、非结构化数据、自定义数据及以上数据类型的混合数据的缓存与交换功能。

应用代理高强度安全交换:用于实现实时请求/响应等应用代理数据交换服务的功能单元,提供主机准入认证、应用进程准入认证、用户身份准入认证、协议分析等高强度安全接入认证功能。

消息服务:用于实现数据收发消息控制的功能单元,提供消息注册服务、数据收发通知服务、告警信息、数据对账服务等功能,为应用系统通过内外网数据安全交换平台交换数据时提供丰富的数据收发控制手段,保障数据收发的可靠性、完整性和实时性。

安全隔离组件用于实现信息内、外网间的逻辑强隔离,并实现逻辑强隔离、身份认证、设备接入认证、协议转换、信息摆渡等安全功能,该组件依据安全策略严格控制信息内、外网间的数据交换,严格控制执行数据交换的接入设备,严格控制数据交换的传输协议,并断开内外网 TCP/IP 网络连接,抵御来自信息外网包括蠕虫攻击、网络攻击、木马攻击、网络嗅探等各类针对信息内网的网络攻击。

边界防护组件用于实现安全隔离交换装置与信息内网之间的逻辑隔离,并执行边界 ACL 访问控制策略,保护信息内网数据区边界安全,实现网络攻击防护,IP 地址、端口、协议和时间访问控制,NAT 地址转换,逻辑隔离等边界防护安全功能。

平台集中管理系统实现对平台的统一管理,包括对使用平台进行数据交换的应用系统进行统一注册管理,对应用系统所有的数据交换任务进行统一任务管理,对应用系统进行的所有数据交换的安全策略进行统一策略管理,对应用系统所有的数据交换过程和内容进行统一安全审计,对平台所有设备的运行状态进行统一监控和管理。

3.2.2　电力企业复杂业务场景下内外网数据安全交换体系设计

内外网安全交换平台的数据交换体系包括数据交换方式和数据收发控制方式两部分。提供了结构化、非结构化、定制协议(半结构化混合类型数据)、高强度安全交换(实时应用请求/响应数据)等多种类型、灵活的数据交换方式,满足电网企业互联网复杂应用场景下不同类型业务数据交换的需要。如下图所示。

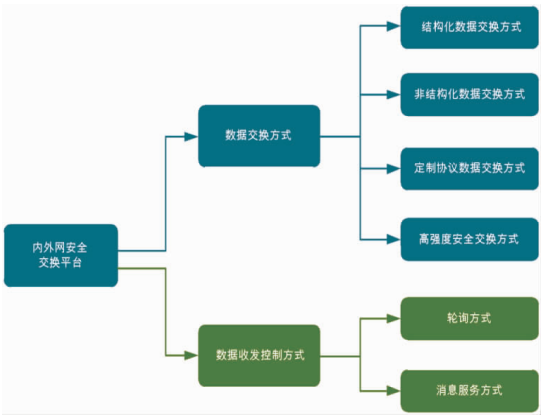

图　数据安全交换体系设计

Fig. 1　Design of data security switching system

数据收发控制方式是指应用系统在使用内外网数据安全交换平台交换数据的过程中,采用适当的方法对交换过程进行控制,确保数据交换的完整性与可靠性。内外网安全交换平台提供两种数据收发控制方式,即轮询方式和消息服务方式,实现内外网网络连接断开状态下应用系统间安全的状态信息交互[11]。

3.2.3 内外网安全防护平台统一安全管理系统设计

内外网安全交换平台设计采用 SNMP 和 SYSLOG 协议,实现对内外网安全交换平台内数据库防火墙、应用数据交换单元、定制协议交换单元、消息服务单元、高强度安全交换单元、数据缓存系统、隔离网闸、防火墙等设备的统一安全管理[12]。主要功能包括:

拓扑管理:对内外网安全交换平台设备拓扑结构进行管理。

设备状态管理:对设备 CPU、内存、网络流量等平台软硬件运行状态进行监控。

内外网数据交换监控:对内外网所有的数据交换过程进行实时监控。

数据交换任务与安全策略管理:统一管理所有管理员配置的内外网数据交换任务与内容过滤、认证等安全策略。

安全告警管理:实时监控平台任何软硬件发送的病毒、非法访问、设备故障等安全告警信息。

安全审计:采集平台所有软硬件设备的系统日志,并提供日志审计功能。

4 电网企业内外网数据安全交换平台应用成效

电网企业在应用了内外网数据安全交换技术后,实现了对电网企业内部网络与互联网出口的统一安全防护能力和安全管理水平,加强了内外网业务数据交换的管控力度,制订了严格的边界安全策略,封堵了各种攻击路径,强化了对数据交换内容的安全过滤。在实现内外网安全隔离防护的同时,满足各类应用系统对内外网数据交换的需求。并实现了以下安全体系[13]:

(1)建立了多级隔离,逐级增强的多层次安全防御架构。从互联网到信息内网依次部署了外网防火墙、IPS、WEB 应用防火墙、数据库防火墙、多类型数据安全交换系统、隔离网闸、内网防火墙等,构成等级化的安全防护体系,全面封堵各类互联网攻击。

(2)建立了丰富的数据交换体系,满足电网企业各类应用系统对内外网数据交换的多样化需求,提供四种数据交换方式,包括采用定制协议交换类型支持半结构化混合类型数据安全交换,满足应用系统对高性能、低延时、混合类型数据交换等复杂应用场景的需求。

(3)创建消息服务机制,实现应用系统与内外网安全交换平台间的有机融合。采用消息服务机制建立内外网应用系统间安全的状态信息交互机制,将应用系统运行状态监控、历史交换数据对账、数据缓存空间告警、数据到达通知、消息队列等技术方法运用到内外网数据交换过程控制之中,在不破坏内外网文件级数据交换安全性的同时,保证内外网应用系统间状态信息的实时交互,保证数据交换的完整性、可靠性。

(4)建立严格的人员与设备安全准入机制和数据交换控制机制,对进行内外网安全交换的主客体实行了严格的管控。采用高强度安全交换机制,实现主机接入的硬件实体指纹 + 应用程序合法性的高强度准入控制,保障了实时应用访问请求的内外网交换安全性,有效防止非法指令请求/应答信息在内外网间传输。集中管控数据交换任务,严格控制内外网数据交换行为、格式内容和方向,保证内外网数据交换的安全性。

(5)建立双链路双活的高性能、高可用性的交换体系,提供应用级负载均衡,结构化数据交换能力 10 000 条/s,非结构化交换能力 50 MB/s,定制协议交换能力 160 MB/s,高强度交换能力800 Mbps,充分保障内外网数据安全交换体系的鲁棒性和交换性能。

5 结束语

随着电力信息化的发展,互联网接入电力管理信息网络的需求越来越迫切,然而来自互联网的攻击手段不断变化、攻击对电力系统造成的破坏越来越严重[14-15]。本文结合电网企业的业务应用特点,参考电网企业相关安全标准以及其它行业内外网安全防护体系的建设思路与方案,设计了电网企业内外网安全防护平台,设计了内外网安全防护体系技术框架、数据交换体系和安全

管控体系,并在某电网企业进行了实践。从实际效果上看,本文设计的内外网安全防护平台和数据安全交换平台满足了各类业务系统内外网数据交换的需求,达到了多级隔离、有效管控的安全防护目标,解决了内外网隔离环境下的数据交换完整性保障问题,验证了性能及可靠性满足电网企业应用系统需求。

来自互联网的安全威胁始终在不断变化,网络攻击对电力正常生产运行造成的影响也越来越严重,因此,今后需要在现有内外网安全交换平台的应用研究基础上,不断加强对电网企业内外网安全防护平台自主可控体系化建设的研究,加强安全态势感知与防御机制智能化的研究以及应用交换行为大数据分析等方面的研究,不断巩固和完善内外网安全交换平台的安全防护能力[16-17]。

参考文献:

[1] 陈瑜. 企业信息安全风险管理的框架研究[J]. 价值工程,2017,36(18):53-55.
CHEN Yu. Research on the framework of enterprise information security risk management[J], Value Engineering,2017,36(18):53-55.

[2] 曹琰. 网络安全威胁因素及其常见网络安全技术分析[J]. 电子测试,2015,0(07):65-66.
CAO Yan. Network security threat factor and its common network security technology analysis[J]. Electronic Test,2015,0(07):65-66.

[3] 王静,高昆仑,张波. 基于网络隔离与安全数据交换的发电集团双网体系研究与设计[J]. 电信科学,2017,33(02):163-176.
WANG Jing. GAO Kunlun, ZHANG Bo, Research and design in dual network scheme of power corporation based on network isolation and secure data exchange [J]. Telecommunications Science 2017,33(02):163-176.

[4] 邓蕴. 基于网络安全的隔离措施分析[J]. 控制工程,2017,(02):2566-2570.
DENG Yun. Analysis of isolation approaches for network security [J]. Control Engineering of China,2017,(02):163-172.

[5] 周瑞珏. 信息共享机制下的网络安全信息界定[J]. 北京邮电大学学报(社会科学版),2017,19(06):54-62.
ZHOU Ruijue. Definition of network security information under information sharing mechanism[J]. Journal of Beijing University of Posts and Telecommunications (Social Sciences Edition),2017,19(06):54-62.

[6] 敖麟钦,陈卓. 基于网络隔离技术的信息资源共享方案研究[J]. 软件导刊,2017,16(06):163-167.
AO Linqin, Chen Zhuo, Research on information resource sharing scheme based on network isolation technology[J]. Software Guide 2017,16(06):163-167.

[7] 程军. 一种新型网络隔离单向传输设备的设计与实现[J],通信技术,2017,(10):2385-2390.
CHENG Jun. Design and Implementation of Novel Network-Isolation and Unidirectional Transmission Equipment [J]. Communications Technology,2017,50(10):2385-2390.

[8] 刘强,蔡志平,殷建平,等,网络安全检测框架与方法研究[J]. 计算机工程与科学,2017,(12):2224-2229.
LIU Qiang, Cai ZHI ping, YIN Jianping, et al, Frameworks and methods of cybersecurity detection[J]. Computer Engineering and Science,2017,(12): 2224-2229.

[9] 陈兴蜀,杨露,罗永刚. 大数据安全保护技术[J]. 四川大学学报(工程科学版),2017,(5):1-12.
CHEN Xingshu, YANG Lu, LUO Yonggang, Big data security technology[J]. Journal of Sichuan University(Engineering Science Edition),2017,(5): 1-12.

[10] 牟明福,苏正泉. 大数据发展的信息安全风险防御探析[J]. 中国安全生产科学技术,2017,13(9): 66-71.
MU Mingfu, SU Zhengquan. Analysis on the risk of the development of big data from thperspective of information security [J]. Journal of Safety Science and Technology,2017,13(9):66-71.

[11] 王景仪. 大数据时代的信息安全分析[J]. 电子测试,2017,(24):110-111.
WANG Jingyi. Information security analysis in the era of large data[J]. Electronic Test,2017,(24): 110-111.

[12] 徐振华. 网络安全态势感知模型设计和实现[J]. 电子测试,2016,03:23-25.
XU Zhenhua. Design and implementation of network security situational awareness model[J]. Electronic Test,2016,(03):23-25.

[13] 张淋江,刘志龙. 基于信息安全的高校风险评估模型的研究与实现[J]. 河南科技,2015,(03):18-20.
ZHANG Linjiang, LIU Zhilong. Research and implementation of university risk assessment model based on information security [J]. Journal of Henan Science and Technology,2015,(03):10-20.

[14] 娄屹萍. 信息安全管理体系换版解析——解读 ISO/IEC27001-2013 信息安全管理体系要求[J]. 标准学科,2016,(08):63-68.
LOU Yiping. Analysis on information security management system——interpretation of ISO/IEC 27001-2013: information security management systems-requirements[J]. Standard Science,2016,(08):63-68.

[15] 杨玥,张胜军,康琪. 基于电网运维数据的智能预警系统设计[J],内蒙古电力技术,2017,35(04):20-23.
YANG Yue, ZHANG Shengjun, KANG Qi. Design of intelligent early warning system based on grid operation and maintenance data [J]. Inner Mongolia Electric Power,2017,35(04): 20-23.

[16] 李爽,刘洋,吴一非. 基于大数据的新型信息安全技术研究[J]. 软件产业与工程,2015. 36(06):31 -35.
LI Shuang, LIU Yang, WU Yifei. The new information security technology based on big data[J]. Software Industry and Engineering, 2015,36(06):31 -35.
[17] 杨英仪. 面向能源互联网的数据一致性框架[J]. 广东电力,2017,30(12):22 -28.
YANG Yingyi. A data consensus framework for energy internet [J]. Guangdong Electric Power,2017,30(12):22 -28.

收稿日期:2017 -12 -08

作者简介:

郭仁超(1990)男,本科,助理工程师,现主要从事贵州电网有限责任公司信息化项目建设工作。

(本文责任编辑:范 斌)

Research on the application of data security exchange technology of internal and external network in power grid enterprises

GUO Renchao[1], **XU Yutao**[2]

(1. Information Centers of Guizhou Power Grid Co., Ltd., Guiyang 550002, Guizhou, China;
2. Electric Power Research Institute of Guizhou Power Grid Co., Ltd., Guiyang 550002, Guizhou, China)

Abstract: In order to protect enterprise secrets, it is necessary to adopt a safe, effective and mature technology to ensure the security of enterprise information. The security equipment, such as the network gate, is the basic data security exchange platform for internal and external network, through network isolation, security access control, protocol stripping, recombination and other technologies to realize controllable and secure data exchange, a set of perfect data security exchange system for internal and external network is established. This article refer to the power grid enterprise security protection standards, the public security information communication network boundary access platform security standards and other industries both inside and outside network security protection design, combined with the application requirements of power grid enterprises, proposes a multi-level security isolation protection, security strategy for strengthening management and control of data exchange, It also designs an internal and external network data security exchange platform, data exchange system and security management control method that meets the needs of power grid enterprises, and realizes security data exchange between internal and external network of power grid enterprises. At the same time, the application effect of the system in the actual environment of the internal and external network of the power grid enterprises is expounded in combination with the pilot, the promotion and the practice.

Key words: network isolation; information exchange; access control; safety management