工程技术与管理 · 第 03 卷 · 第 06 期 · 2019 年 08 月
DOI: https://doi.org/10.26549/gcjsygl.v3i6.2119

Analysis on Security Risks and Countermeasures of Power Plant Information System

Yan Yang　Aimin Yu

Huadian Qingdao Power Generation Co., Ltd., Qingdao, Shandong, 266031, China

Abstract

With the continuous deepening of the application of information technology in China's power plants, power generation companies are increasingly dependent on information systems and networks, and the importance of information security is becoming more and more important, which also places higher demands on information security and information professionals on the power plant side. This paper analyzes the safety risks and countermeasures of power plant information systems, and aims to provide reference for personnel engaged in information work in power plants.

Keywords

information system; security risk; prevention strategy

浅析电厂信息系统安全风险及对策

杨燕　于爱民

华电青岛发电有限公司，中国 · 山东 青岛 266031

摘　要

随着中国电厂侧信息技术应用的不断深化，发电企业对信息系统和网络的依赖程度越来越高，信息安全的重要性显得愈加重要，这也对电厂侧的信息安全和信息专业人员提出了更高的要求。本文对电厂信息系统存在的安全风险和对策进行了分析，旨在为电厂从事信息工作的人员提供参考。

关键词

信息系统；安全风险；防范策略

1 引言

近年来，全球发生多起因信息安全造成的停电事件，影响比较大的诸如 2010 年伊朗核燃料工厂遭遇“震网病毒”袭击，导致控制系统失效 1000 台离心机损坏。2014 年美国俄亥俄州核电站受到蠕虫病毒攻击，网络数据传输量剧增导致系统变慢，控制计算机连续数小时无法工作。2015 年乌克兰电网遭遇黑客攻击，直接造成约 70 万个家庭在圣诞前夜陷入一片黑暗。根据统计截止 2016 年全球已发生 300 余起针对工业控制系统的攻击事件。其中电力行业发生的工控信息安全事件占比达 20%。[1] 在中国工业化的进程中，发电厂对信息系统的依赖程度越来越高，提升了企业生产自动化水平，但我们必须认识到，信息系统和网络是一把双刃剑，给企业信息安全带来了巨大的挑战。我们必须识别出电厂信息系统所面临的各种风险，并做好相应的应对策略。

2 目前电厂信息系统面临的安全风险

2.1 物理风险

物理风险主要指信息网络硬件设备所面临的各种安全风险，如雷击、火灾、电磁干扰、人为破坏等，其会直接导致设备的损坏，造成难以弥补的损失。发电企业的信息系统面临的物理风险主要集中在信息中机房建设、环境安全、基础设施等方面，导致信息系统的可靠性、安全性不高。

2.2 网络风险

网络风险是指信息网络面临的病毒及黑客威胁，尤其是开放的网络，更是容易受到外部的攻击和入侵，入侵者可以利用系统中存在的安全漏洞，针对电厂信息网络进行恶意攻击，从而导致网络的瘫痪，机密信息被篡改或者窃取。[2] 在实际工作中，有些电厂因为资金或者管理不到位等种种原因，

没有严格遵循等保要求，在控制区、非控制区和管理大区之间部署相应的隔离装置，或者存在防火墙缺失，核心交换机选型不合理、管理大区发生 ARP 攻击等，都是电厂比较常见的网络风险。

2.3 系统风险

随着信息化水平的提高，电厂使用的信息系统越来越多，如果某一个系统中存在漏洞受到黑客的攻击或感染病毒，就会引起连锁的反应。因此，系统风险会形成巨大的安全隐患，一旦被利用，将会给电厂带来不可估量的损失。

2.4 数据风险

电力系统的数据风险可能存在于数据的存储、处理和传输整个过程中，主要体现在数据存储、传输的安全性和真实性上，[3] 数据可能丢失，也可能被人为地截取、篡改或者破坏。

2.5 管理风险

近几年，信息安全这一课题已经提升到国家层面，各行各业也愈加重视，但是很多电厂的管理者在思想认识上还有一定的局限，认为信息是为企业生产服务的，对信息系统的安全重视不够，很多发电厂或多或少都存在以下风险：信息化安全机构建设尚不健全、信息和网络的管理机制不健全、网络安全设备升级改造进度滞后、计算机用户的信息安全意识和保密意识有待提升、信息和网络安全教育培训不到位等问题。

3 电厂信息系统安全防范策略

电厂必须强化对信息系统的安全防护工作，可以从物理安全、网络安全、系统安全、数据安全和管理安全这几个方面入手，制定相应的安全防范策略。

3.1 物理安全

物理安全是信息系统安全的前提，主要包括场地安全、设备安全、介质安全，从机房设计之初，就应当严格遵循国家标准进行设计。

3.1.1 场地安全

场地安全即机房的安全，可以从以下几个方面来考虑，即供配电系统、防雷接地系统、消防报警及自动灭火系统、门禁系统、监控系统和机房环境综合监控系统。

3.1.2 设备安全

设备安全包括设备的防盗防毁、防止电磁信息泄露、防止线路截获、抗电磁干扰一级电源的保护。

3.1.3 介质安全

介质安全是要保护存储在介质上的数据，包括介质本身的安全和数据安全。目前电厂信息系统备份方式除了备份服务器外，主要还是采取移动硬盘来进行数据的备份。介质安全的目的是保护存储在介质上的信息，对于介质本身来说，主要是保证介质的防盗、防毁、防霉、防丢失、防潮等。

3.2 网络安全

威胁电厂网络安全的威胁来自各个方面，有计算机系统本身的不可靠性、环境干扰以及自然灾害等因素引起的，也有人为操作引起的，只有消除了所有的安全威胁，网络才是绝对安全的。但任何一个网络，要完全消除各种威胁和隐患，是不可能的。因此，采取积极有效的防御措施是保证网络安全的前提，需要技术和管理并重。

3.2.1 做好安全分区

电厂必须要严格遵循等保的要求，划分控制大区、生产大区和管理大区，并且在区域边界部署防火墙和网闸等网络安全设备，这样可以有效地杜绝外部攻击并且保证控制大区和生产大区的网络安全。

3.2.2 部署网络安全产品

网络安全产品包括防火墙、入侵检测设备、堡垒机、安全审计设备、网闸等，作为电厂的信息专业，应当尽可能部署各种网络安全产品，一方面是符合等保的要求，另一方面可以最大程度地保障电厂信息系统网络安全。最大可能全面部署等保要求的人的精力是有限的，再优秀的员工，也无法做到 24 小时实时在线去管理网络、识别风险，最大化地利用好网络安全设备和技术，才能更好地保证电厂信息系统的安全。

3.3 系统安全

为保证系统安全，必须安装服务器版的杀毒软件外，还可以配置堡垒机提升访问控制，配置服务器系统提升操作系统本身的安全性，需要特别注意的是，在操作系统补丁升级之前，必须经过严格的兼容性测试验证才能安装补丁升级包或更新软件，[4] 以防止更新补丁导致系统蓝屏、崩溃的情况

工程技术与管理·第 03 卷·第 06 期·2019 年 08 月
DOI: https://doi.org/10.26549/gcjsygl.v3i6.2119

出现，影响系统的正常使用。

3.4 数据安全

从信息安全发展趋势来看，信息安全防护的核心都将归终于数据安全，因此对于电力行业而言，保护电力数据安全是电力信息安全核心内容。[3] 电力信息系统运行过程中无论发生任何突发状况，电力信息系统数据多需要保证其完整性，确保数据信息不会发生丢失、泄露和损坏。[5]

3.4.1 保证数据的保密性

数据在交互和传输过程中，采用身份认证、端到端加密、线路加密以及更强的应用层协议进行综合防护。对数据的访问用户进行统一管和授权，防止未经授权的用户非法获取数据，对可疑访问进行阻断，确保电厂信息系统的数据不被非法截获。

3.4.2 保证数据的完整性和可用性

保证数据的完整性和可用性，即要确保数据不会因为各种风险因素被修改、删除、破坏，哪怕因为地震、火灾等不可抗力的因素导致服务器发生故障或者损坏，只要有可还原的数据备份副本，电厂的核心数据就不会丢失。在配备专业的备份硬件后，应当根据应用软件的不同，从完全备份、增量备份、差异备份当中选择适合的备份方式。另外，在有条件的情况下，尽可能实现异地备份，以对抗不可抗力情况的发生，保证信息系统的数据安全。

3.5 管理安全

一个企业的信息系统不管硬件部署的再固若金汤，如果员工的能力和素质不够，企业管理有漏洞，那么再强大的系统也形同虚设。信息安全的所有问题，追根溯源，都可以归结到管理上，可以在机构设置、规章制度、教育培训等方面下功夫。

3.5.1 完善信息机构设置

许多电厂信息部门不是独立的部门，有的附属于生产技术部，有的设置在办公室，有的缺乏规范的建制和岗位，这种状态往往导致信息工作不受重视、相关工作推进缓慢。信息专业是一项系统工程，必需要完善信息机构设置，才能与电厂的各生产专业、各职能部室进行密切配合。

3.5.2 明确职责分工

电力企业采取安全分级负责制，明确安全防护的主要责任人与相关人员管理责任，按照“谁主管谁负责，谁运营谁负责”的原则进行安全管理，各级计算机和网络设备的安全管理由所属单位负责，并相应设置监控系统和网络安全专职管理人员。[6]

3.5.2 做好标准制度建设

电厂应当结合自身实际情况，优化信息安全管理流程，制定出适合本企业的信息化工作管理标准、信息网络管理标准、信息系统安全管理标准、应用系统管理标准、计算机及办公设备管理标准、信息机房管理标准等信息方面的企业标准，规范信息安全管理标准和制度建设，对信息系统安全提供强有力的制度支撑和管理保障。

3.5.3 加强人员教育培训

人是信息系统中最不稳定、最不确定，也是最危险的因素，特别是内部人员，是信息安全的最大威胁。近年来，其他国家电厂发生的几个重大信息安全事件，追根溯源，问题都归结在企业内部人员的不安全行为上。因此，电厂应当加强对信息人员和用户的思想教育、职业道德和技术培训，防止人为主观入侵事件的发生，并有效阻止外来非法访问、非法入侵。信息安全人员管理教育的对象，应当包括与信息安全相关的所有人员，不仅是信息专业技术人员，还应当涵盖企业领导和中层管理人员、DCS 系统运维人员、普通计算机用户及其他相关人员。通过一系列培训、管理和保密教育，提高发电厂员工信息安全防范意识，建设一支遵纪守法、精通本职业务的信息安全技术队伍，这是做好发电企业信息安全基础。

4 结语

笔者在电厂从事信息专业已经 10 余年，深感国家、行业、集团对信息安全越来越重视，要求也越来越高，随着信息安全技术网络安全等级保护基本要求、国家能源局 36 号文、网络安全法等国家标准和法律法规的实施，集团公司、省调和企业内部从上到下都愈加重视，市网警支队也会经常到企业内部进行督导和检查，信息安全工作有了很大的提升。然而，如同企业的安全生产工作一样，信息安全同样不能有丝毫懈怠，不存在绝对安全的系统和网络，绝不能盲目乐观。电厂的信息安全是一场旷日持久的保卫战，也是一个动态的过程，需要在工作中根据实际情况进行持续的完善改进，对信息人员的专业水平和职业素养提出更高的要求，需要付出持之以

恒的耐心，保持加倍的使命感和责任感，守卫住企业的信息安全！

参考文献

[1] 尹峰 . 浅析电力企业工控系统风险和防御 [J]. 大众用电 ,2017(S1):148-150.

[2] 陈海平 . 广州蓄能水电厂信息网络安全建设 [J]. 通讯世界 ,2015(12):110-111.

[3] 聂元铭 , 朱卫国 , 刘世栋 . 电力信息系统数据安全防护 [J]. 信息安全与通信保密 ,2015(04):45-47.

[4] 李田 , 苏盛 , 杨洪明 , 文福拴 , 王冬青 , 朱林 . 电力信息物理系统的攻击行为与安全防护 [J]. 电力系统自动化 ,2017,41(22):162-167.

[5] 王林信 , 栗志鹏 , 王刚 . 云计算背景下的电力信息系统数据安全 [J]. 电子技术与软件工程 ,2019(11):204.

[6] 席明湘 , 闫江毓 , 吕英杰 , 邓博仁 . 电力信息系统安全研究 [J]. 警察技术 ,2014(S1):59-61.