电力信息安全的技术措施和管理方法

张海宁　张冲

国网天津静海供电有限公司　天津　301600

[摘　要]近年来，网络黑客等势力不断入侵居民的网络安全系统，使得居民越来越关注网络信息安全问题，电力部门作为事关国计民生的重要部门，其信息安全也受到社会各界的关注。电力信息安全直接影响着电力部门的正常运行，在信息安全问题日益突出的当下，改进电力信息安全技术与管理方法已经刻不容缓。

[关键词]电力信息；安全措施；管理方法

【DOI】10.12252/j.issn.2096-627X.2021.10.115

一、我国电力信息管理存在的问题

1.1信息安全管理系统尚待完善

当前我国电力信息安全系统还存在许多缺陷，主要表现在不同部门的信息共享程度不高、软件系统设计存在漏洞等方面。在需要人工进行统计、记录的环节，还存在数据记录不明确、信息化程度低、信息使用效率不高等问题，因此，完善我国电力信息安全管理系统是当前必须解决的首要问题。

1.2软硬件技术落后

我国电力系统的发展与完善经历了一个较长的周期，这使得我国电力系统的软硬件设施在很大程度上依赖于国外的先进设备，且长期以来，我国对电力信息系统的重视程度不足，这使得与电力信息系统有关的软硬件技术迟迟得不到发展。在大量使用国外先进技术的情况下，我国电力信息系统缺乏自主性，也缺乏基本的安全性，这不利于保障我国的电力信息安全，要改变这一现状，必须加大科技投入，形成我国拥有独立知识产权的电力信息系统。

二、电力信息安全的技术措施

2.1网络防火墙

防火墙是企业局域网到外网的唯一出口，这里的外网包括到不同安全层次的电力网、其他信息网如政府网和银行网络、Internet，所有的访问都将通过防火墙进行，不允许任何绕过防火墙的连接。DMZ停火区放置了企业对外提供各项服务的服务器，既能够保证提供正常的服务，又能够有效地保护服务器不受攻击。要正确设置防火墙的访问策略，遵循“缺省全部关闭，按需求开通的原则”，拒绝除明确许可外的任何服务，也即是拒绝一切未予准许的服务。与Internet连接的防火墙的访问策略中，必须禁止Rlogin，NNTP，Finger，Gopher，RSH，NFS等危险服务，也必须禁止Telnet，SNMP，TerminalServer等远程管理服务。

2.2物理隔离装置

主要用于电力信息网的不同安全区之间的隔离。物理隔离装置实际上是专用的防火墙，由于其不公开性，使得更难被黑客攻击。

2.3入侵检测系统

入侵检测系统是专门针对黑客攻击行为而研制的网络安全产品。国际上先进的分布式入侵检测构架，可最大限度地、全天候地实施监控，提供企业级的安全检测手段。在事后分析的时候，可以清楚地界定责任人和责任事件，为网络管理人员提供强有力的保障。入侵检测系统采用攻击防卫技术，具有高可靠性、高识别率、规则更新迅速等特点。系统具有强大的功能、方便友好的管理机制，可广泛应用于电力行业各单位。

所选择的入侵检测系统能够有效地防止各种类型的攻击，中心数据库应放置在DMZ区，通过在网解决电力信息安全的技术措施和管理措施络中不同的位置放置，比如内网、DMZ区网络引擎，可与中心数据库进行通讯，获得安全策略，存储警报信息，并针对入侵启动相应的动作。管理员可在网络中的多个位置访问网络引擎，对入侵检测系统进行监控和管理。

2.4网络隐患扫描系统

网络隐患扫描系统能够扫描网络范围内的所有支持TCP/IP协议的设备，扫描的对象包括扫描多种操作系统，扫描网络设备包括服务器、工作站、防火墙、路由器、路由交换机等。在进行扫描时，可以从网络中不同的位置对网络设备进行扫描，扫描结束后生成详细的安全评估报告，采用报表和图形的形式对扫描结果进行分析，可以方便直观地对用户进行安全性能评估和检查。

三、电力信息安全的管理措施

3.1信息安全教育。安全意识和相关技能的教育是企业安全管理中的重要内容，其实施力度将直接关系到企业安全策略被理解的程度和被执行的效果。为了保证安全的成功和有效，高级管理部门应当对企业各级管理人员、用户、技术人员进行安全培训。所有企业人员必须了解并严格执行企业安全策略；主管信息安全工作的高级负责人或各级管理人员，重点是了解、掌握企业信息安全的整体策略及目标、信息安全体系的构成、安全管理部门的建立和管理制度的制定等；负责信息安全运行管理及维护的技术人员，重点是充分理解信息安全管理策略，掌握安全评估的基本方法，对安全操作和维护技术的合理运用等；信息用户，重点是学习各种安全操作流程，了解和掌握与其相关的安全策略，包括自身应该承担的安全职责等。当然，对于特定的人员要进行特定的安全培训。

3.2人员管理。保持信息人员特别是网络管理人员和安全管理人员的相对稳定，防止网路机密泄漏，特别是注意人员调离时的网络机密的泄漏。对网络设备、服务器、存储设备的操作要履行签字许可制度和操作监护制度，杜绝误修改和非法修改。

3.3密码管理。对各类密码要妥善管理，杜绝默认密码，出厂密码，无密码，不要使用容易猜测的密码。密码要及时更新，特别是有人员调离时密码一定要更新。

3.4技术管理。主要是指各种网络设备、网络安全设备的安全策略，如防火墙、物理隔离设备、入侵检测设备、路由器的安全策略要切合实际。

3.5数据管理。数据的备份策略要合理，备份要及时，备份介质保管要安全，要注意备份介质的异地保存。

3.6加强信息设备的物理安全，注意服务器、计算机、交换机、路由器、存储介质等设备的防火、防盗、防水、防潮、防尘、防静电等。

3.7注意信息介质的安全管理，备份的介质要防止丢失和被盗，报废的介质要及时清除和销毁，特别要注意送出单位修理的设备上存储信息的安全。

3.8客户端的防病毒软件不得随意卸载，要及时更新病毒代码库。

四、结语

总之，我国电力信息安全系统还存在许多问题，技术人员必须对我国电力信息安全系统进行持续观察研究，并适当汲取外国的先进经验完善自我，为进一步加强我国电力信息安全奠定良好的技术基础。我国科研部门还应当加强对电力信息安全技术的研究，尽快脱离对国外技术的依赖，形成具有我国自主产权的电力信息安全系统。

参考文献

[1]孙剑.电力大数据信息安全分析技术研究[J].华东科技：学术版，2017（10）：272.

[2]赵微微.电力信息安网络安全防护领域当中安全隔离技术措施得到的应用[J].城市建设理论研究：电子版，2017（23）：166.

[3]李鹏.电力大数据信息安全技术研究[J].低碳世界，2016（23）：51-52.