Universe Scientific Publishing
Hydropower and Water Resources 水电水利
第 2 卷◆第 10 期◆版本 1.0◆2018 年 10 月
文章类型:论文 | 刊号(ISSN):2529-7821

浅析电力信息安全存在的问题及解决对策

张斌龙
上海格蒂电力科技有限公司西安分公司
DOI:10.32629/hwr.v2i10.1568

[摘　要] 随着信息时代的到来,信息安全已经融入电力企业生产经营活动的方方面面。由于电力信息安全在电力企业发展中具有重要影响,而且多是通过网络传输协议进行数据传输的,因此在数据传输和信息共享的过程中,还存在很多的漏洞,而且容易受到不法分子的攻击,会对我国整体电力企业产生不利的影响,因此必须及时发现在电力企业信息安全管理中存在的问题,并积极地采取措施,保证我国电力信息的安全,保证电力企业的顺利发展,为我国国民经济的发展做出重大贡献。本文分析了当前电力信息安全存在的问题,并提出了解决对策。
[关键词] 电力信息安全;问题;对策

1 简述我国电力系统中的信息安全技术

1.1 信息访问安全技术的设置

电力系统信息在被访问的过程中, 其大量的信息比较容易泄露和丢失。因此做好电力系统信息访问过程中的风险防范相当重要。在互联网普及的年代,为了加强网络信息的安全性,大部分信息技术系统都会设置实名认证环节。因此, 对电力信息系统进行身份认证是降低其风险性的有效途径。身份认证技术是要求对系统进行访问的人员进行实名认证,系统通过辨别访问人员身份信息的真假,对恶意采用假身份进行访问的人员进行有效阻止。在身份认证技术全面普及的局势下, 我国电力系统的风险性得到了有效控制。其次,我国电力系统设置了访问控制技术,这种技术的主要目的是防御系统中那些不合法的信息访问。当系统中的信息被访问时,如若访问内容出现越权行为,系统就会自动采取防御措施,阻止访问继续。由于电力系统中的信息被越权访问,是造成系统陷入风险的重要因素,因此,对越权访问行为直接进行访问拒绝, 是有效保证信息系统安全的关键措施。

1.2 信息访问安全

(1)身份认证技术:这种技术就是访问者向系统表明身份,首先系统要对访问者的身份进行识别,识别就是看访问者是谁,在识别后对开始验证工作,而验证就是证明访问者的身份是否真实。而识别验证的过程就需要,系统能够自动对每一个访问者的身份进行识别, 而且访问者的身份要合法,这样才能使识别的工作有效。在电流信息系统中,使用比较广泛的身份认证技术,就是口令以及数字认证。

(2)访问控制技术:保证信息系统安全关键的工作就是访问控制,访问设置决定了是否可以访问或者是直接拒绝。在安全信息中会出现越权使用信息的情况, 而访问设置就是出现越权的时候,进行自动的防御。越权可能引起风险,因此要对这种行为防御,以免出现风险。用户只能允许的范围内,行使权利去使用信息,绝对不能越权,访问控制主要有两项工作,一个是授予权利,另外一个就是对访问的用户鉴别。

(3)安全审计技术:安全审计技术是不可缺少的技术,主要是控制系统中的人员以及设备, 并且在控制后可以得到证据,而且证据是电子的形式,这种审计技术是为了防止二次破坏的系统。使用安全审计系统可以对系统中的数据记性记录,及时的掌握数据的变化,而且能识别事件是否安全,并且事件进行定位。

2 电力信息安全存在的问题

2.1 物理安全风险

物理安全风险是指电力系统的硬件设备以及通讯链的安全,例如路由器、交换机,以及各种服务器。其风险来自多方面,例如闪电和洪水等自然灾害,可能会导致硬件设施被破坏,导致用户信息丢失,产生损失。人为的破坏或者失误性操作也是重要的原因。另外,服务器里的数据库系统、操作系统等也存在着各种各样的漏洞, 这些漏洞同样存在着很大的安全风险。

2.2 网络安全意识差

近几年电网的发展极其迅速, 电力信息化建设快速成长, 而电力信息化安全系统的建设却远远没有跟上前者的脚步,导致很多安全隐患的出现。虽然很多企业都开展了信息安全风险评估工作, 但是大多数都是借鉴外国的信息安全评估体系,没有创新,不能与企业自身的信息安全系统很好的融合。有很多评估工作都是按照国家的基本要求开展,只针对某个安全问题单一的检查加固,缺乏整体性。

2.3 备份恢复技术差

备份恢复技术, 也称为业务连续性技术或灾难恢复技术。无论做出怎样的防护措施,都只能把安全风险尽量降低,不能完全排除发生意外的可能。无论出现上述哪种情况,都有可能丢失数据,造成很大的损失。如果没有良好的备份恢复技术,损失将不可挽回。很多电力企业备份恢复技术差,出现意外后无法完全将数据恢复。

2.4 生产管控系统中存在的安全风险

为了使企业的各个部门能够有条不紊地进行生产,必须保证各部门之间信息的畅通。在电能产生、传送、分配、调

度等全过程中应保证电力信息的安全，保证信息系统的正常运行。在电网的实际运行过程中,需要对电网调度自动化系统、变电站自动化系统、电厂监控系统等电力企业的基本运行系统进行信息安全的保护工作，因为这些系统也是最容易受到不法分子攻击的系统。随着电力企业的不断发展,原有的电力系统正往可靠性越来越高、实用性更强的方向发展,因此在电力信息的内容也在不断地丰富当中,原有的静态的生产控制系统已经转变为以工业以太网为控制基础的动态管理阶段，因此对电力信息安全方面的要求也越来越高了，但是生产控制系统的实际运行情况却并不理想,还经常出现由于冒充、窃收、重放或是篡改等现象,进而导致控制系统的信息安全受到了很大的破坏，还影响了电力管控系统信息之间的传输和共享，在电力管控系统调试和维护的过程中，部分人员在商业利益的诱导下还容易在管控系统中植入恶意的代码或是程序，不仅影响电力管控系统的信息安全,对电力系统的整体运行也产生了消极的影响。

3 加强电力信息安全的对策

3.1 强化身份鉴别

保护电力信息安全,在提高电力系统安全方面,可从准入方面加强安全力度，对进入电力企业网络系统的身份进行识别。可以发挥网络识别的作用,来判断用户是否具有操作权利。应用身份鉴别技术时,一般以动态口令的方式。即便此种鉴别方法专业技术性并不是非常高，但操作较为方便,可引入到电力系统中。电力企业的内部员工只要具备用户名与口令密码，并经相关人员核对后就可进入电力信息系统中,从而保护电力信息的安全。当然,在具体操作中,需要将其他的加密技术应用于电力信息系统准入机制中,以便更好地保护电力信息安全。

3.2 提高防病毒的水平

随着电力行业的发展,电力系统经营、发展及管理的各个方面都离不开计算机技术，但是计算机在自身发展过程中容易受到病毒的入侵,病毒具有隐蔽性、潜伏性等特点,所以如果电力系统内部的操作人员不及时采取措施进行预防和维护,电力企业的信息就会受到威胁。为了提高电力信息的安全，必须保证信息和数据在传递及共享过程中的安全性,安装正版的防毒软件,进行定期的杀毒。在电力系统内部,为了保证信息安全,可以建立专门的计算机病毒预防和监督控制中心,聘请专业的计算机人才,负责这项业务,对电力系统中的病毒进行分层防范，最终提高电力系统的安全,保证电力系统的正常运行。

3.3 完善信息化管理的标准规范

在信息化建设过程中，技术平台与信息编码的构建,需要制定统一的标准作为支撑，才能保证信息管理系统中的各个子系统顺利地进行信息关联。在不同的电力企业当中,对信息化建设的要求与着眼点不同，这就要求相应的信息化标准也要具有针对性,在实际构建过程中,需要保证信息化组织构建、数据信息的统一,同时也要保证标准化的关键信息,能够对企业各个部门与组织进行相应的管理。通过健全信息化管理的标准规范,将企业管理者、电力员工以及业务操作连成一体,从企业整体规划的角度统筹规划,从基层业务着手实施优化与调整措施，将企业的信息资源进行有效整合,从而实现信息化建设过程中的系统集成,并利用信息标准化,实现资源整合与系统集成的贯彻实施。

3.4 建设安全管理支撑平台

建设安全管理支撑平台,能够完善信息安全管理,实现安全管理工作从分散到集中的跨越，为构建电力系统的整体安全防护体系打下基础，保障电力信息系统的安全稳定运行。安全管理支撑平台应成为统一管理体系的技术和流程支撑,通过定期漏洞扫描和配置脆弱性核查,能感知信息系统的安全脆弱性和安全防护能力，通过收集安全设备日志等进行关联分析，能将安全事件和风险实现可视化展示,使管理人员能及时了解全网安全状况和安全发展趋势,实现安全态势可感知。

4 结束语

总之,电力信息系统的建设大大提高了运营效率,提高了相关企业的效益。在快速建设电力信息系统的同时,更要注重电力信息安全系统的建设。保护电力企业信息安全是非常复杂而且重要的工作。保护基础硬件设施,防止数据丢失。加强生产管理系统的建设,防止生产系统被恶意破坏,产生不必要的损失。提高网络安全意识,让企业的安全风险评估工作落实到位,不流于形式,全方位提高电力信息安全。

[参考文献]

[1]陈志新,华晓.剖析电力信息安全中网络日志审计系统的作用[J].大科技,2014,(12):39.

[2]王凤彬.信息安全技术在电力信息系统中的应用分析[J].现代国企研究,2015,(11):56.

[3]王舒.电力企业网络信息安全现状与分析[J].电脑知识与技术,2016,(09):39+43.