浅析电力监控系统网络安全加固技术

李勤琴
（国网重庆市电力公司垫江供电分公司，重庆 408300）

摘 要：新时期发展背景下，电力行业作为推动我国经济持续发展的关键部分，在居民生活以及生产力水平持续提升的现状下，更加对电力提出了更多的要求。为了能够做好广大群众高质量的用电服务工作，那么在电力企业经营生产时，做好监控网络安全防护以及安全加固处理工作极为关键。文章以电力监控系统为出发点，针对电力监控系统网络安全加固技术提出了几点建议，希望能够给相关人士提供重要的参考价值。

关键词：电力系统；监控；网络安全；加固
【DOI】10.12231/j.issn.1000-8772.2020.33.201

1 引言

对于电力监控系统来讲，一方面时监督企业高效电能生产的基础上，另一方面也是维持电能安全传输的保证。作为我国电力企业经营中不可缺少的部分，这就要求企业必须实施妥善的监控系统网络安全加固操作。通过妥善的网络安全加固处理技术，降低监控系统运行中一切危险因素，致力于我国电力企业经济效益不断提高的效目标当中。

2 电力监控系统定义

针对人们生活以及生产中不可或缺的电能结构，在我国电力企业持续发展中，自动化、数字化时代的到来，一定程度上也推动电网系统更加完善，不管是企业所进行的电能生产，还是电能传输等多个工序，都必须始终围绕电力监控系统进行。分析电力监控系统，作为电力企业生产中的核心部分，就是整合了计算机等现代化的技术手段，对企业生产以及电能供应等多个环节实施监督的系统结构。

3 电力监控系统网络安全加固技术

3.1 网络及电力二次安防设备加固

当前企业所应用的电力监控系统，行业人士按照网络结构差异性，将其合理的划分为生产控制与管理信息两个单元，分析内部各个细节，主要涵盖路由器、防火墙以及交换机等多个内容，虽然所有单元之间独立运行使用，但是相互之间只有加强联系，才能够构成完善电力监控系统的同时，营造安全性的网络运行氛围。在企业实施该部分加固处理时，可以将工作重心放在物理与逻辑两个层面下，秉持与时俱进的发展理念，及时升级换代各个软件，结合企业日常经营管理问题下，事先制定好妥善处理方案，最为重要的是，也应该找出安全性极高的区域，切实维护好系统良好的运行环境。详细分析网络及电力二次安防设备加固技术处理，此时工作人员可以从以下几个方面进行处理：第一，在电力企业日常网络安全加固处理过程中，企业经常使用的就是调整管理方案以及安装补丁等手段，工作人员事先先对电力二次安防设备性能进行分析，因为不需要企业投入较大的经济量，再加上极高运行效率等优势，在加固操作过程中，这就需要工作人员借助最小的权限，将 IP 地址及端口进行妥善开放，同时，置顶黑名单与封堵高危端口，像核心的业务部分，也应该构建加密通道，及时进行各个软件的升级换代，整合一系列的措施，构建安全性的网络运行环境；第二，适当的增加完善的硬件设备。特别是在新时期发展基础上，市场上出现了很多现代化的网络安全技术，为了能够提高网络抗风险能力，工作人员将网络进行有效的增加或者是修改。具体操作时，站在网络边界部分，将入侵防御系统进行合理增设，在生产控制和管理信息大区部署网络安全态势感知装置、移动介质管控平台及防病毒管理中心[1]。

3.2 主机操作系统加固

在硬件与应用软件之间，作为电力监控系统最核心的布恩，操作系统的存在，当前主要应用的就是 Windows 和 Linux，在较多版本类型下，像之前企业所应用的比较落后的操作系统，当前已经没有针对性的技术作为支撑。鉴于电力企业网络运行氛围下，呈现出了一定的特殊性，一旦不能实时更新网络系统，在常规安全补丁性能下，就会导致系统出现一系列的弊端，再加上系统没有良好的杀毒软件，自然威胁到网络安全、稳定运行的基础上，无形之中也会对电力企业造成严重的影响。面对以上问题下，在企业实施主机操作系统加固处理时，可以整合身份鉴别、安全审计、资源控制等多个部分实施妥善操作，详细操作步骤如下：第一，身份鉴别：所谓的身份鉴别，主要就是围绕账户与口令，对该部分实施全方面的加固，像存在的默认账号，可以严禁使用；而多余的账户，也可以进行彻底删除；在工作人员设置口令时，也应该尽可能的复杂化；第二，安全审计：针对安全审计工作而言，主要就是面对启用操作系统，对其日志审计性能进行研究，详细记录好登录以及访问等多个环节产生的数据信息；第三，资源控制。在登录系统时，主要就是要求锁定其设备终端操作超时行为；第四，访问控制。通过访问控制实施主机操作系统加固处理过程中，主要涵盖的就是系统服务、端口以及共享等几个部分。详细的操作流程，就是禁用 Web、telnet、Email、FTP、rlogin 等不必要的高危服务，关闭 135、137、138、139、445、3389 等高危端口，禁用匿名远程连接与远程访问注册表路径和子路径，关闭默认共享功能；第五，入侵防御。通过入侵防御手段，安装系统补丁，然后做好安装工作，重点进行恶意代码保护工。实际操作过程中，由专业技术人员先对系统性能进行测试，如果处于正常状态的系统兼容性，在接下来就可以将系统补丁进行有效的安装，尤其是一些不需要使用的应用软件，彻底的清除，之后完成最小化系统安装工作。面对当前多种手段病毒侵蚀手段下，工作人员可以将恶意代码软件进行妥善的安装，而像一些不能安装防恶意代码软件主机系统，此时工作人员可以应用杀毒 U 盘[2]。

4 结束语

简而言之，经过较长时间观察可以看出，针对电力监控系统网络安全加固技术来讲，在企业内部人员实际应用过程中，体现出了动态性等的特点，因为涵盖了较多的数据信息，这就应该要求企业维护好系统安全性极为重要。面对各界人士多样化用电需求下，科学技术提高衍生出很多攻击手段，在电网结构迈向数字化、智能化方向中，要想能够确保电力监控系统更加稳定运行，电力企业就应该做好网络及电力二次安防设备以及主机操作系统等方面的加固处理，提高系统使用价值，为我国电力企业尽快实现可持续发展目标打下坚实的基础。

参考文献

[1]孙佳炜，朱红勤，潘小辉，等.基于主机操作系统的检测与加固实现[J].机电信息，2018(36).
[2]张喜铭，李金，邱荣福，等.国密体系在智能变电站的研究与应用[J].南方电网技术，2020，14(1).