电力企业网络信息安全的防范措施

林　昀
福建省福能海峡发电有限公司　福建　福州　350200

摘　要：伴随着整个社会不断发展，对大数据的应用愈来愈多，可以说大数据是时代发展的助推，社会发展各行业的发展与大数据的应用紧密联系，而大数据又必然随着网络来用，仅有有效运用网络才能更好的充分发挥大数据的功效。因而要确保网络的安全性才能够为大数据的发展给予稳定靠谱的渠道。现代企业几乎都设立了内部结构网络信息管理系统，根据网络数据共享平台调研市场的发展动态性，使企业能够得到全新市场前景，获得核心竞争力。电力企业是国营企业，服务平台包含诸多我国电网商业秘密，要进行网络安全管理的范畴比较大，需要处理审批的数据信息比较多，容易受网络黑客和病毒感染等威协，危害公司的经济收益，乃至给公司产生很严重的财产损失。怎样做好安全防范管理方法，需电力企业依据电网的发展，进行研究和分析。

关键词：电力企业；网络信息；安全防范

引言：伴随着信息系统和互联网的迅猛发展，作为关联国计民生的企业，电力工程企业的结构业务数据基本都是在互联网上流通，企业对信息系统的依赖非常大。但企业享受信息系统带来极大的经济收益的前提下，正面临着相对较高的风险性。如果出现数据泄露或数据篡改，能给国家和企业带来不可估量损失。2016年11月7日《中华人民共和国网络安全法》[1]施行后，网络信息安全已经达到了国家安全与创新发展的相对高度，网络信息安全变成头等大事。因而，作为供电公司，我们应该再次应对现阶段安全问题，寻找高效的预防措施。

1 电力企业网络信息安全的意义

现阶段，我国电力系统已经与网络信息系统高度连接，网络数据能不能安全工作直接关系着电力系统的稳定运行。但结合实际，信息网络系统属性存在一些难题，其信息安全维护比较弱，电力系统非常容易遭到侵略和个人信息泄露等安全问题。信息安全主要原因是日常网络安全管理中安全隐患问题，最后导致顾客信息泄露出去。除此之外，电力系统运行中，管理者在工作期间不可以严格管控变电器、发电机组配电设备等特色，导致网络信息安全事故，最后导致电力系统出故障，不能正常运行。

2 电力企业网络信息安全的现状分析

2.1 防范措施不足

伴随着电力数据信息网络信息化管理变成电力应用管理中不可缺少的设备，电力数据信息网络兼具了信息化管理工作与精准同步控制工作中，电力管理和电力制造的联络离不开电力信息内容网络运转的支撑点。伴随着信息内容技术的发展和网络技术性的发展，网络发案率逐年递增。电力目前已经基本设立了对应的网络信息安全管理体系，但公司内部网络内容在员工管理、消毒系统软件、密钥管理、验证、数据信息传输加密、员工安全防范意识等多个方面依然存在众多安全隐患。从全部电力信息内容网络来说，不少企业网络的信息安全存有不均衡、网络使用率高、安全隐患多等难题，特别是安全标准相对较低的经营风险比较高。比如，美国乔治亚州 Hatch核电厂2号发电机组出现了全自动断电。那时候，一位技术工程师正在更新工厂业务流程网络的计算机技术以搜集操纵网络临床诊断数据信息，以同步业务流程网络与控制网络间的数据和信息。技术工程师重启电子计算机后，同步程序流程重设了操纵网络的统计数据，自动控制系统忽然减少了原子炉贮水池的水位线，自动退出整个发电机组。因为缺乏防范措施，未能及时合理[2]。

2.2 员工安全意识有待加强

现阶段，中国电力公司员工的安全防范意识良莠不齐。 比较之下，年青员工和领导者的安全防范意识比较高，但中老年人员工和一线员工依然欠缺必须的安全防范意识。主要是参加工作时间、文凭、信息安全水平学习程度、工作内容等多种因素所造成的。 这为网络安全性留下风险。提升电力公司的信息安全，全方面的提升员工网络信息安全观念能够避免信息安全保障的误差。

2.3 网络硬件存在风险

首先，磁盘和硬盘是用以存放信息的主要物质，可是磁盘和磁盘的厂家许多，品质也良莠不齐，假如难以

保证磁盘和电脑硬盘的品质，则存放的信息可能丢失，无法保证互联网信息的完好性。另一方面，存储介质就会受到环境因素或人为因素产生的影响。比如，在暴风雨期内或者在电磁波辐射强度大的环境里，因为无线电波产生的影响，存放的信息会丢失或存储介质很有可能毁坏。人为因素主要是因为人为失误造成信息丢失所引起的设备常见故障[3]。

2.4 电力系统的设备软件安全存在漏洞问题

由于有关新科技设备的管理方面万一存在的问题，就很可能造成信息产生泄露从而引发一系列负面影响，因此为了降低设备管理者的工作中压力，手机软件管理工程师经常会在设备开发环节设定信息安全出口。该安全出口能够给信息一定日常维护功效，但是因为技术实力比较有限，其本身也有许多不够。参考信息人工智能的科学研究结果显示，大概60%的木马程序均运用该安全通道进行计算机进攻实际操作。鉴于此，现在的开发商在发布新科技电子器件设备后马上给该设备加设修复作用，为此提升电子器件设施设备安全运营。

3 电力企业网络信息化的安全建设要求分析

3.1 数据的完整性

在供电系统的信息互联网建设中，信息数据的存放和传送必须严苛安全性。 因为在储存或传送期内删不掉或变更，因而全部数据可能遗失并且不详细。除此之外，在软件更新环节中，还改善了信息系统软件，在存放信息时具备检测与审批作用，防止了人为因素粗心大意所造成的信息泄漏忍不安全隐患。

3.2 数据的可控性

管理人员核准的合理合法访问者可以按照单位操纵，但是必须避免对于整个数据库控制作用。这将会保证访问者数据利用的一致性和可选择性。

3.3 访问的安全性

根据网站访问的消费者也要获得管理人员的批准才可以查询与处理数据。 禁止表明违法访问者和非法访问者的数据。这不但非常容易损害标注的数据，并且对互联网信息安全与全部资源池构成威胁，抑止互联网信息化的高速发展。

4 电力企业网络信息安全的防范措施

4.1 全面规划电力信息安全管理目标

电网遮盖普遍，电力企业本身包括大量业务数据和设备运行信息。为了能高效地管理方法大量的信息数据信息，最先要高度重视电力企业的内控机制。电网信息平台上的安全系数涉及到电力用户本人的信息和个人隐私。由于电网上连接着银行或公安机关信息认证管理系统等。假如客户本人信息被泄漏，人身财产的安全性就会受到威协。因而，供电公司的信息安全工作风险大，都是电力运行全面的缺点。计划和建立相应的安全管理目标，有利于电网信息的全方位维护。电力企业要做好管理方法，机构不一样单位的信息融合，设定地区分布式系统支系安全扣，中控台总公司加强监管，全方位评定企业大数据服务平台信息风险性，做好木马程序和网站渗透安全防护。使得信息保护与检测单位可以阶段性分析与清除安全隐患，保证电网信息的全局性维护监管[4]。

4.2 重视安全教育

人们常说“凡事预则立不预则废”意思就是 ”即公司以人为本的核心原则，把塑造员工安全意识作为防范公司网络信息安全的关键方式。但安全防范意识和安全素养离不开职位支撑点，总体上规定电力企业将各岗差别融进工作内容和职位要求等数据，切合实际、针对性地开展职工网络信息安全防范文化教育活动。 因而，在具体防范环节中，有关电力企业应该具有关键、层次分明、有终点开展网络信息安全防范专业知识。职工网络信息安全防范的综合能力水准理应塑造自身的安全性防范观念，根据专业知识等形式产生企业特色的网络信息安全防范气氛，并纳入企业制度建设的思路。

4.3 对信息系统的安全风险进行评估

电力工程企业信息系统是一个巨大而繁杂的技术架构。在实际世界里，巨大繁杂的信息管理系统不可避免存在易损性，换句话说存在信息安全风险。在这样的情况下，需要通过适度、全方位的安全防范措施将剩下风险降到最低。 要进行所谓风险分析与风险评定、剖析电力工程企业信息系统所面临的风险、剖析信息管理系统遭遇危胁、处理问题或把它剩下风险降到可以接受的水准。针对电力企业而言信息安全评定是电力工程企业信息系统的工作现阶段信息安全相关工作的客观性需要与急需解决是制定安全战略的根据。

4.4 加强漏洞扫描技术的应用

（1）信息安全性漏洞扫描。信息存放是计算机基本要素之一，但会带来许多风险性。电子计算机信息存放主要是由客户实际操作。计算机系统漏洞有可能在储存环节中导致用户信息遗失或泄漏，严重威胁个人信息安全。因而，为了防止信息存放过程的信息泄漏威协，利用漏洞扫描技术扫描信息安全性漏洞尤为重要。此外，信息安全性泄漏主要是由监管、拷贝息息相关的个人行为等故意个人行为造成，因而信息安全性漏洞进攻主要是由人即时手动式开展。（2）扫描病毒感染漏洞。病毒入侵是电脑网络信息安全中最常见的、最具影响力威

协。进入计算机后，计算机系统将停止运行，网络空间安全性将大幅度降低。除此之外，扫描网络病毒漏洞至关重要，因为大部分病毒入侵都不容易检测与解决。病毒攻击计算机系统开展攻击方式主要通过传送数据安全通道，尤其是在下载文件的过程当中病毒感染非常容易侵略计算机系统。因而，确保传送数据安全通道安全性是十分重要的。应用常规漏洞扫描技术扫描电子计算机信息安全通道，可以有效的预防病毒根据传送数据安全通道进到计算机系统，并查验计算机系统存不存在病毒感染漏洞。（3）扫描垃圾短信。垃圾短信通常是客户烧录进到计算机，再次搔扰客户。因而，必须采用漏洞扫描技术来监控全部下载的软件程序流程，查验是不是带有垃圾短信并传出警示[5]。（4）扫描通讯漏洞。现阶段，互联网是世界最大的通讯系统。但另一方面，很多恶意程序和病毒感染利用通讯系统的漏洞专用工具来利用计算机系统。尤其是当客户连接到网络时，也会产生对应的信息流。从而为病毒感染和恶意程序进攻带来了较好的机遇。大家电脑上打开互联网和软件时，经常遇到制导技术式弹夹。这也是漏洞。当客户点击“明确”时，病毒软件和病毒感染将荣获操作权限并受到伤害。

4.5 完善网络安全制度

要从根源上彻底保证网络安全，尽量提高供电系统安全生产工作，在日常工作中完善网络安全管理体系，在规章制度管理人员工作职责中最大限度地处理安全风险。建立和完善信息管理系统。企业要加强我们在日常工作中使用网络严格管控，避免员工在办公室里电脑上下载不良信用记录。这不仅会对所有区域内的企业办公室气氛，而且病毒性感染会探寻切入点，给信息管理系统造成损坏。一部分大中小型硬件设备的运用务必申请办理备案，使整个运用整个过程清晰度，防止人为因素泄露硬件信息，降低全局性安全隐患。硬件和设备严格监管务必技术专业开展进行维修人。硬件机器设备交易运送需要有人监管。引进设备后，务必专业技术系统开展设备调试，从而实现整体网络安全检查。审核后，连接硬件信息管理系统。在硬件机器设备公布运用之前，一定要进行风险评价。供电系统企业设立了风险评估工作组，每个部门主要从用过和未用过的硬件作出评价和检查，分析安全风险和风险类别，最后依据贴标签差别硬件安全防护水平，在操作流程职工开展硬件型号规格所选择的后，对作业人员的专业素养展开剖析此外，供电系统还需要提升和激励团队责任感，避免心理状态松懈造成的不良影响和严重危害。

结束语：文中根据研究，意识到为了实现稳定发展的需求，电力企业将网络信息安全视作确保必要条件之一，搭建完备的电力企业网络信息安全防范管理体系，充分运用对于工厂生产及行业发展的缓冲作用，持续创新技术理念促进企业内部网络信息安全系统软件刷等级，为切实解决实践中所存在的困难制定系统化及完好性解决方案。总得来说，电力企业网络信息安全防范服务体系是一项长久性及复杂度的工作步骤，总体上规定有关专业技术人员认真细致看待设计任务综合考虑设计方案方案的可行性及可执行性，不可怀着一劳永逸的观念开展下一步工作，为推进在我国电力企业持续发展打下好基础。

参考文献：

[1]牛斐.电力企业网络信息安全的防范措施[J].大众用电，2020，305（S1）：168-169+180.

[2]易磊磊，赵博.电力企业网络信息安全的防范措施研究[J].低碳世界，2020（26）.89-90.

[3]赵建辉.浅析电力企业信息网络的安全及防范措施[J].通讯世界，2020（22）：178-179.

[4]白文远，张宪康.论电力信息网络安全的防范措施[J].数字技术与应用，2021（12）.202-203.

[5]吴艳.电力信息网络安全结构及存在的入侵问题[J].科技传播，2021（19）：234-234，223.