

电力信息安全问题分析与防范措施研究

周磊

国网雅安电力集团公司

[摘要]随着我国对网络信息建设投入的不断加大,我国的信息化水平也在不断提高,但是由于计算机网络的开放性及其本身固有的脆弱性,导致各种网络安全事件屡见不鲜,直接或间接地影响了企业的信息安全。电力企业是关乎国计民生的基础性行业,一旦其信息泄露或是信息被篡改等,造成的损失会严重影响到国家的安全、社会的稳定。本文分析了网络信息安全的基本内涵、电力信息安全存在的问题,并提出了提高电力信息安全的措施。

[关键词] 电力信息; 安全问题; 防范措施

[DOI] 10.12252/j.issn.2096-6288.2021.10.840

引言

现在的社会已经是一个信息化的社会,当然,在信息化不断发展给人们带来了诸多便利的同时,也有很多的问题在不断的产生。信息的安全问题尤其是一个特别重视的问题,信息安全方面存在着很多的漏洞,使得信息在不断的泄露,也有很多的网络入侵问题,导致信息被盗,这些都给信息安全带来了很大的问题。

一、网络信息安全的基本内涵

信息安全是指防止任何对数据进行未经授权访问的措施,或者防止造成信息有意无意泄露、破坏、丢失等问题的发生,让数据处于远离危险、免于威胁的状态或特性。网络安全是指计算机网络环境下的信息安全。因此网络信息安全就是指计算机网络信息系统的硬件设备或者软件极其重要数据信息受到保护,不因突发事件或者恶意破坏而遭到损害、更改或者泄露,从而使网络信息系统能够连续安全运行。

二、电力信息安全方面的常见问题

(一) 信息网络管理机制不健全

随着大数据时代的到来,各行各业对于数据的建设越来越有经验,移动互联网技术的发展带给了人们随时随地上网的便利,信息流通速度快,人们在不受时间、地点的限制下浏览着各类信息。虽然开放式的网络环境帮助人们更快的了解周围的时事,但是众多的信息混乱在一起很难分辨,电力企业并不是只有简单的记录和规划人们的用电情况,电力企业也需要了解民生动态,信息的混乱导致电力部门无法真正的了解民生情况,严重影响了电力部门的工作效率。而且电力企业的一些负面信息一旦被发现有迅速在网络上传播开来,届时电力企业无法掌控舆论的走向,导致对电力企业部门失去信心将会造成更大的损失;而且信息网络管理的机制不健全会使信息的传播与实际工作的衔接不及时,很多重要信息有时候无法以最快的速度传达到用户的身边,网络舆情无法有效控制和解决。

(二) 员工信息安全意识薄弱

从以往电力信息事故来看,数字信息的管理人员也是一项重要的安全威胁因素,其主要原因就是管理员工的安全意识不足,认为电力信息在电脑中不会有任何的风险。而且很多事故的发生就是因为一些管理员工的错误操作造成的,在面对一些有危险性的邮件或者文件时没有足够的警惕意识,结果导致计算机被一些木马程序或者病毒控制,大量的电力信息被窃取。虽然我国对电力信息的安全问题很重视,并制定了相关的法律法规来约束管理员工,但是并没有引起人们的足够的重视,导致管理员工的意识薄弱。

(三) 缺乏专业的技术人员,监管不到位

人才无论何时何地都是被需要的,电力部门在信息安全保护工作上无法真正的做到万无一失,还是因为相关的技术人员的技术能力不够。而且更多的企业在网络的使用上花费了大量的人力物力,使计算机收集和统计信息的能力越来越强,但是在网络的安全防护上却没有投入足够的精力,从而出现了越来越多的网络问题。同时还有一些电力企业对计算机网络的监管也不到位,对于不是自己研发的服务器往往是

听之任之,网络运行中存在着极大的安全隐患也没有察觉,反而继续让这些服务器工作,还没有任何的安全防护措施,认为运营商会做好服务器的安全防护工作,结果出现了很多的网络安全事故。

三、电力信息安全的防范措施

(一) 建立健全管理机制

建立健全监管机制,强化相关管理部门维护公共安全的功能,让网络信息安全的各项制度都能够发挥其职能,在落实现有监管机制以及法规的前提下,通过各种技术手段打击非法行为,加强信息保密机制、设施改建,增强网络在各种可能发生情况的应急能力,提高网络的安全性、可靠性以及保密性。除此之外,还应该协调各部门之间的管理职能,整合各部门,形成合力,共同筑建网络信息安全防护体系。对于舆情管理,除了高度重视,建立健全舆情管理机制之外,还应该构建网络预警机制,提升网络信息的管理能力及技术水平,通过改进技术管理,净化网络世界。

(二) 加强对员工安全意识的培养

管理人员是电力信息安全防护的一道大门,为了确保这道大门的有效性,必须提高管理员工的安全防护意识,因为他们是每天检测信息安全程度,以及是电力信息出现问题时第一接触人员,所以他们的相关技术和基础素质必须要合格,为了确保管理员工的能力,对于一些管理员工必须遵守的法律法规,必须有相关的课程让其学习,还要不定期的对管理员工进行相关技术的培训,确保安全管理工作能够顺利的进行。除了电力企业内部管理员工的安全意识需要培养,中国上亿的网民也应该得到足够的网络安全教育,提高自己的法律意识以及在上网时的安全意识,不能盲目的跟风随大流。

(三) 加强技术更新以及对技术骨干的培养

电力企业在加大网络信息安全管理投入的同时,除了不断完善、更新网络安全防护设备,还应将重心转向专业技术人员培养。从外外引进专业技术人才,为单位注入新鲜血液。加大对技术人员的培训力度,定期对其进行培训,保持知识的更新以及技术的更新。不断地更新建设,并且保持其安全、可靠。总之,除了加大对网络信息安全的外部管理,还应从内部进行防御,建筑一道难以被攻破的围墙,把一切可能发生的安全事故都隔绝在外。

结束语

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。保护电力企业信息的安全是非常复杂而且重要的工作。加强电力信息管理的建设,防止信息系统被恶意破坏。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] 李源浩. 电力信息网络安全风险分析与防护策略研究[J]. 分析仪器, 2021(4): 4.
- [2] 谢汉明, 米雪峰. 电力信息安全技术防护措施探讨[J]. 电工技术, 2020(17): 2.