信息化建设中网络安全与维护策略探究

焦梦天
国电河南新能源有限公司　河南　郑州　450000

摘　要：近年来，在我国信息技术飞速发展的背景下，各行各业纷纷开展了信息技术的应用，利用网络信息技术提高企业的经济效益，降低人力和物力资源的消耗。然而，伴随着科技的进步，信息化建设的过程中，网络的安全问题频频发生，变成了一个巨大的隐患，并且网络安全问题也将对各行业造成极大的影响，因此，专业技术人员必须对电力企业中的网络安全问题进行持续剖析，积极探索解决网络安全隐患的策略，维护信息化建设中的网络安全。

关键词：信息化建设；网络安全；维护策略

随着社会经济的快速发展，信息化建设为生产生活提供了便利。享受便利的同时，也要对网络安全加以重视。由于网络的不安全因素，会使电力企业中计算机遭到病毒袭击等问题[1]。在信息化建设过程中，各种软硬件问题都会造成网络安全隐患，而网络安全问题所导致的损失也是难以估量的，所以，有关工作人员必须在重视网络安全问题的基础上，高效开展信息化建设，切实维护电力企业网络安全。

1 信息化建设中网络安全与维护风险与挑战

1.1 网络安全面临巨大信息挑战

随着电子信息科技的快速发展，企业所面对的管理问题越来越严峻，同时，科技的飞速发展的今天，部分电力企业对网络安全管理越来越滞后，因此，企业的网络安全管理也越来越复杂，这就需要对企业的网络安全管理给予足够的关注。随着越来越多的公司开始运用信息化建设，改善公司的经营与管理，公司对信息技术的信心也越来越高，这让网络帐户安全性受到极大的威胁。目前，我国电力企业普遍面临着严重的信息泄漏问题，而这类企业忽略了对网络的安全性研究，从而导致了企业资金流失。许多企业因为缺少资金和技术的支撑，都在进行信息化建设项目，而对网络的管理和预防却一点效果都没有，导致很多的网络安全问题的出现，给社会带来了巨大的经济损失。网络安全技术具有交互性的特点，要想成功地处理各种安全问题，需要有关工作人员不断加强信息系统安全管理能力。信息化建设在现代的基础设施和信息技术的支撑下，运用信息资源与信息技术方法，建立起一种能够有效地利用信息资源、高速传输与处理信息，提升工作效能与经济效益。

1.2 企业所面临的安全风险研究

网络安全是对信息资源进行有效保护的一项重要工作。信息化建设的快速发展与广泛应用的今天，互联网已经逐渐成为人们获取信息，进行信息交流，进行商务活动的一种主要方式。在信息技术与互联网蓬勃发展下，企业信息化的进程越来越快，同时也带来安全风险。企业对网络信息的安全性缺乏足够的重视，因为其独特的业务工作方式，企业在对其进行内部的经营管理时，往往将重点放在生产经营方面，而对公司的信息安全性却没有给予足够的重视。在应用过程中，网络安全遇到多种威胁，比如黑客入侵，电脑病毒感染，数据泄漏等，在我国企业信息化建设进程中，网络的安全问题越来越突出，它们将给电力网络以及信息系统带来很大的危害，并给社会到来危害或是经济损失。

2 信息化建设中的网络安全与维护现状

2.1 网络管理员缺乏网络安全意识

随着互联网的广泛应用，行业相关人员网络安全意识的认识不够深入，因此，对各行业的网络建设中进行各类攻击、恶意侵入也越来越多。随着信息技术的发展，各行各业的工作内容都越来越离不开互联网，与之相对应的是，信息系统面临着各种不同类型的安全隐患，面临着严峻的挑战。但是，事实上，在我国的信息化建设过程中，各行业在应用过程中信息安全防护意识一般都比较薄弱，网络安全系数也比较低[2]。大部分的网络管理员和使用者对网络安全的管理都没有深刻认识。由于没有足够的安全防护手段，无法避免黑客通过网络体系中的弱点进行攻击，病毒入侵或其它的安全威胁，只能依赖于防御软件来抵抗外界的攻击，这给网络的稳定、持久的工作带来了潜在的风险。

2.2 缺少有效的网络安全防控方法

近几年，世界上各个国家的科技进步突飞猛进，同时，网络安全入侵者的高科技手段也越来越多，给网络资源带来了极大的危害。网络安全入侵者的攻击目标是非法的，破坏者攻击对于网络安全而言，都是带有敌意

的，比如：在攻击过程中，网络安全入侵者更改正常使用者的权限，导致正常用户无法登陆，或是故意破坏、盗取电脑中的资料，这样就造成了很大的网络安全隐患。另外，当前的木马病毒、蠕虫病毒等对电脑中的数据造成了很大的危害，这种病毒一进入电脑，就会对电脑的运算速度造成很大的伤害，并且可以无限地进行拷贝，最终造成电脑的瘫痪，给整个网络的安全带来了巨大的风险[3]。由于缺乏多个层面的反应机制，所以难以形成一个高效的网络安全防护联动体系，这也是网络安全管理过程中，很可能会遇到安全防护问题的薄弱环节，从而引发信息安全方面的问题。

3 信息化建设中的网络安全与维护问题的策略

3.1 建设网络安全数据库系统

在企业信息化的网络体系中，包含了大量的数据库，这些数据库主要是作为存储和管理信息的。如何保证数据库系统的安全性和机密性仍然是各电力企业最为关注的问题。在当今社会，由于计算机与互联网的飞速发展，使得数据库在现代社会中起着举足轻重的作用。数据库就是存储并处理与计算机相关的资料的系统，也就是说，数据库既可以存储各类数据档案，也可以存放软件包含的程序。数据库系统的作用就是通过特定的方法来实现对各种业务数据的存取；具备对数据库的管理与操作，能够让用户和应用程序对数数据进行访问，并且对相关数据管理与维护。网络安全就是以保障已有资源为前提，运用成熟的安全防护技术与方法，来实现网络安全目标[4]。由于网络安全技术具有多样性、交互性等特点，如何在不同的应用环境中有效地解决这些问题，对信息安全管理提出了更高的要求。网络安全就是保护网络系统免受非法访问、使用、泄漏、破坏、篡改等多种威胁的能力。随着信息技术的发展与普及，网络已经成为人们获取信息，进行数据交互的重要途径之一。同时，网络安全建设与维护也是时代发展的要求，要根据信息建设中出现的问题，积极寻找解决办法，对不良影响因素进行解决。

3.2 企业信息化平台管理层面维护

企业信息化的网络安全问题，首先要做好防范的工作，在构建平台时，必须要完善网络安全管理体系，从企业信息化平台的资源上来说，硬件设施、服务器、安全的存储设备、安全管理系统等方面，都应该尽可能地增加资金投入力度，保证企业的信息安全。对于网络的运行与维修，管理人员要做好相关的例行维修工作，保证系统的平稳运行，并且要建立一套严密、高效的网络故障处置机制及突发事件预案[5]。从企业信息化平台的管理方式来看，企业可以在网络管理部门设立一支专职的管理团队，对企业的用户资料进行统一管理，成立一个网络安全核查工作组，对企业信息化平台上的人员流动定期监测。在此基础上，加强对企业信息平台的管理和维护，增强员工对网络的安全性认识。建立一套系统化的网络安全管理标准，还要在企业信息化平台上做好员工筹备计划，主动引入和培训信息技术人才，同时也要借鉴相关的先进经验，利用部门化的管理体制，把网络安全问题整合，并予以解决。在企业的信息化建设中，要保证企业的信息系统不存在任何的漏洞。另外，企业还可以通过高技术手段将公司的内部与公共网络进行分离，在公共网站上进行信息的公开，并对其进行采集内部网络信息，以此来提高公司信息化平台的防御能力，并对公司的数据信息进行安全保护。信息化建设的不断变化发展下，人们的日常生活都离不开网络，与此同时，也存在着一些不可忽视的问题，比如人为的恶意破坏、病毒的非法入侵，会造成一些关键的信息泄漏和损失，这对网络安全正常运行造成了很大的冲击。增强网络安全保护的功能，强化网络安全保护的技术与管理，增强用户的安全意识与网络不良因素的应变能力，进而达到网络安全目标。

3.3 企业信息化平台安全层面管理

企业信息化建设过程中也涉及到了网络的安全问题，因此，必须做好企业的信息安全管理工作，制定有效的信息安全保障措施。首先，可以通过设置高质量的安全保护软件来增强企业的网络安全性。在选购安全产品时，一定要结合企业的实际状况，理性地选用，不要盲目地从不法厂家处购买，这样才能保证网络安全。安装360安全卫士、腾讯电脑管家、金山毒霸等计算机程序，要自主进行创新，在网上进行安全管理的工作，并能对病毒进行快速的检测和清除，进而了解网络的状况，及时应对出现的问题[6]。在企业信息平台内设立网络管理员，对企业信息系统中的各种设备和业务进行全方位的监测和管理。其次，可以通过对互联网的进出口控制，实现对数据流量的控制，对企业的信息系统进行有效的管理。对公司内的局域网设备及其附属设施实行全方位的监测，保证网络的正常运转和安全。最后，平台要对操作员的轨迹进行监控，一旦发现异常情况，要及时沟通解决，在企业信息化平台的管理过程中，要定期与企业员工沟通，提高员工的网络安全意识[7]。

3.4 企业信息化平台信息泄露后处理

企业信息化平台上的信息泄漏后，处理网络安全问题要注意防患于未然，企业更要正视，一旦企业信息化

平台出现问题，给企业带来的损失，企业在信息平台上的个人隐私受到侵害时，是对问题本身视而不见，还是采取保密措施。企业应当认识到，企业自身无法掌控和规避的网络安全问题，应当采取相应的措施来保证企业的信息安全。企业安全管理部门只有以一种积极、正面的态度来对待网络安全破坏情况，与影响信息化建设问题做斗争，注重使用网络的安全保护技术。企业建立应急网络问题处理工作组，在网络出现问题时，迅速作出反应。企业的信息安全管理部门要从不同的方面，制订完备的应急预案[8]。信息安全管理部门可以与技术人员沟通，寻找最佳的办法解决问题。在遇到网络攻击或黑客进入，要及时采取相应的应对措施，以保障自身的信息安全。面对日益复杂多变的信息环境，构建一支素质高、专业技能和经验丰富、年龄结构合理的专业网络安全维护团队，对于保证信息化建设的正常运转具有重要意义。通过完善人员组织结构、合理配置人员、注重人才培养以及建立良好的合作模式，来维护网络的安全性。同时，还要提高安全技术人员的安全意识和风险责任意识，提高对网络安全管理工作的综合分析、网络安全出现风险的判断和执行能力，进而保障信息化建设中的网络安全，利用各种手段维护网络安全性[9]。

结束语：总而言之，在目前我国的信息化建设中，网络安全与维护已成为一个不容忽视的问题。在互联网快速发展的同时，网络的安全性也越来越重要，网络中不良因素会对社会和个人造成了巨大的危害。为此，相关技术人员必须在信息技术发展过程中，强化信息系统的安全性，制订相应的战略与维护对策，以增强信息系统的安全。维护网络的安全性是一项持续性工作，专业技术人员必须随时更新与改进，确保信息化建设的顺利开展。

参考文献

[1]陈庆华.信息化建设中网络安全保护方案设计研究[J].智慧健康,2023,9(17):1-4.

[2]张佳丽.网络安全应与信息化同步规划、建设和运营[N].人民邮电, 2023-03-09(003).

[3]布英塔.网络信息安全现状及对策研究[J].信息与电脑(理论版), 2023,35(03):224-226+230.

[4]孙继东.信息化建设网络安全与防护问题探讨[J].电子元器件与信息技术,2023，7(01):217-220.

[5]黄彪.探究信息化建设中的网络安全与防护策略[J].网络安全技术与应用,2022,(12):104-106.

[6]韩国梁.信息化建设中网络安全问题的研究[J].石河子科技,2022,(05): 76-78.

[7]周健.新时代背景下数字信息化建设的安全问题[J].数字技术与应用, 2022,40(09):217-219+224.

[8]谢宝建.信息化建设中网络信息安全对策思考[J].电子技术与软件工程, 2022,(17):14-17.

[9]杨豫;符鹏;陈鸿君.企业信息化建设中的网络安全管理问题[J].中小企业管理与科技,2022,(09):47-50.