电力网络信息系统的安全风险分析

刘波

明源电力集团有限公司科技分公司,四川 德阳 618000

摘要：电力网络信息系统属于 Internet 与 Intranet，以及 Extraet 系统，所以应用时较为复杂。由于 Internet 接触的范围较广，所以会受到较多风险影响，因此需要展开全面性分析，构建出安全性较高的体系，才能够提高电力网络信息系统整体的安全性。想要解决电力网络信息系统的安全风险，应该对能够涉及的安全风险进行分析，掌握安全风险的实际情况，才能有效解决存在的安全风险隐患。该文章对电力网络信息系统的安全风险分析，并提出相关的解决建议。

关键词：电力网络信息系统；安全风险；分析

引言

电力企业可以根据网络信息系统的结构，对系统与应用方面进行分析，了解系统与应用情况后，制定出有效的安全风险应多措施，降低安全风险的发生概率，保障电力网络信息系统安全运行，为电力企业构建出安全的信息环境，对于电力企业的可持续发展具有重要意义。

1 物理层安全风险

首先，系统环境安全风险。在电力网络信息系统运行的过程中，容易受到火灾事故与水灾事故，以及雷电事故等安全风险影响，不仅会造成电力网络出现中断现象，还会导致系统瘫痪和数据被毁情况，严重的影响到电力网络信息系统的运行。同时如果产生接地不良与机房屏蔽性能较低的情况，容易受到外界电磁与静电的感染，不利于系统的稳定运行。另外如果电力设施与配套设施存在缺陷问题，会引发不同的故障产生，严重影响到电力网络信息系统。由于机房安全设施的自动化技术较为落手，难以对系统的运行与工作状况进行实时监督，无法及时有效发现与解决安全风险[1]。

其次，物理设备安全风险。在电力网络信息系统运行阶段中，会投入较多的网络设备，其中便具有交换机和路由器等相关设备。同时服务器涉及的范围比较广泛，由 PC 服务器与小型机移动设备组成，设备在正常运行的阶段中，如果安全性较低，难免便会对电力网络信息系统与网络应用带来风险影响，如路由器设备出现信息泄露，都无法保证信息的安全，间接地危害到电力企业的发展[2]。

2 网络安全风险

首先，网络体系结构安全风险。电力网络平台作为应用系统建设的主要平台，其中的体系结构与安全机制的设计等环节，会对网络平台的安全性造成直接影响，从而危害到电力网络信息系统的运行稳定性，并降低群众的电力体验。电力网络可以划分为广域网和局域网，分别由 Intranet 与 Extranet 等部分组成，这也导致网络体系结构涉及的内容复杂，如果不同的环节出现问题，都会影响到电力网络信息系统的运行。在运行办公网与业务网，以及 Internet 网的过程中，如果不注重隔离工作，并且网段的划分不科学，以及路由器出现错误与网络容量不合理等，都会对电力网络信息系统的安全带来严重风险，对于信息系统的运行具有重要影响[3]。

其次，网络通信协议安全风险。在电力网络信息系统运行的阶段中，如果网络通信协议存在安全漏洞问题，不仅会造成信息泄露，还会影响到信息系统整体的运行稳定性。由于网

络通信协议具有安全漏洞问题，黑客便可以利用网络设备，以及协议安全漏洞等渠道，对网络进行攻击与信息获取，难以保障群众信息的安全性。比如在没有经过授权的情况下，对业务网络对业务系统进行非法访问，然后再对群众的口令密码与通信密码获取，会直接危害到网络系统的安全性。黑客通过对网络系统漏洞开展全面性扫描后，便会根据漏洞的特点，对通信线路与网络攻击，容易造成网络线路产生拥塞和瘫痪情况，直接危害到电力网络信息系统的安全[4]。

再次，网络操作系统安全风险。在运用网络操作系统时，不管是 IOS 与 windows，还是 Unix 等，其中都具有多样性的安全风险，如路由器与交换机，以及防火墙等环节，都会直接影响到操作系统的安全，容易造成网络处于风险的状态，严重影响到信息系统的运行。最后，Internet 自身安全风险。由于 Internet 属于全球性公共网络，所以涉及的范围比较广泛，因此在数据信息传输的阶段中容易出现延迟与差错，而且无法进行有效的控制，这便会导致数据传输出现错误和中断，造成网络信息的发布较为滞后，与实际情况不符合，难以解决群众的信息需求。同时网络的传输口令密码，以及通信密码等，会被黑客进行截取，然后再篡改和重发到网络，影响到群众的网络体验[5]。

3 系统安全风险

首先，操作系统安全风险。操作系统安全属于系统安全管理的核心，会对系统的安全带来影响。由于 WEB 服务器数据仓库服务器与外部数据交换服务器，以及门户服务器和办公客户机等相关设备的操作系统，主要以 NT 和 Unix 为主，但其中如果存在安全风险，便容易造成信息出现泄露，间接地降低群众的使用体验，这也是出现较多的安全风险问题[6]。

其次，数据库安全风险。数据库是业务应用和决策支持，以及行政办公与外部信息系统的的重要部分，产生的数据信息应该进行保护，避免信息出现泄露的状况，因此应该制定出统一的数据备份，以及恢复机制，然后再对数据库开展全面性管理，可以提升数据库整体的安全。如访问控制和敏感数据安全标签，以及日志审计等环节，都应该提高这些环节的安全等级，缩小系统出现安全风险的概率，构建出安全与牢固的数据环境。随着科学技术快速的发展，虽然电力数据库管理系统能够达到较高的安全级别，但是仍旧存在着较多严重的安全漏洞，能够直接影响到电力数据库管理系统的运行。同时不同的应用系统软件在数据安全管理设计阶段中，也会出现相关的安全缺陷问题，所以相关人员应该对数据库与应用安全性能展开综合性的评估，以此预防给数据库受到安全风险影响，有助于提高数据库系统的安全性[7]。

最后，黑客入侵安全风险。黑客入侵安全风险是由内部与外部组成，而内部指的是入侵人员采用 Sniffer 程序的优势，对网络进行扫描与分析，以此找到系统的漏洞，然后再对内部网络攻击和入侵，达到影响系统运行稳定性的效果。而外部分线是指入侵人员通过对网络的检测，以及木马方式等，对群众的信息数据获取，然后再通过群众的身份进入到系统中，以此获取价值较高的信息数据，从而导致系统出现终止服务的现象，严重危害到群众的使用体验。因此相关人员应该对内部和外部网络进行有效隔离，防止信息数据产生泄露的状况，有助于保障信息数据的安全性。此外还应对外网发出的服务申请进行筛选，仅允许正常通信的数据包进入到相关主机，而其他的服务请求需要拒绝，以此降低系统受到安全风险影响的概率[8]。

4 应用安全风险

首先，身份认证与授权控制安全风险。相关部门可以采取动态动态口令和 CA 第三方认证的形式，加强系统的安全性，这也是较为先进的认证形式，虽然具有较高的安全性，但是

操作与管理出现不当的情况，都会引起安全风险发生。因此需要对应用服务和信息系统展开全面分析，构建出具有统一性的身份认证与授权体系，可以有效识别不同访问人员的信息情况，然后再给予访问者相关权限，可以防止利用他人信息入侵的风险发生。

其次，信息传输完整性安全风险。在不同的情况下，工作人员与用户会将重要的传输到 Internet，这也导致 Internet 性能会直接影响到传输的效果，如果没有做好传输工作会导致信息数据出现不完整，以及出现非实时可能性，也给黑客创造入侵的机会。因此便可以将 Internet 的 SSL 虚拟专用网络作为基础，然后再利用传输加密与电子签名手段的优势，对信息数据传输安全性不断提升，以此降低相关的安全风险发生。

最后，实时信息作为应用系统的核心信息内容，因此必须要提升信息传输的机密性防止信息数据出现泄露。而想要实现安全传输的目标，可以融入加密方式与密码算法和密钥管理等形式，不断提升传输的安全等级。相关部门通过全面性分析后，可以利用密码管理委员会和公安部批准的加密方式、密码算法和密钥管理的方式，对这一环节安全不断加强，以此保证应用系统的安全性较高，能够长期处于稳定与安全运行环境。

5 管理层安全风险

管理人员作为网络设备管理的核心，能够直接影响到网络设备的安全性，所以相关部门应该认识到管理环节的重要性，不仅需要构建出专业性较高的管理队伍，还应该对管理造成的安全风险进行分析，然后再制定出有效的安全措施，有助于降低安全风险的产生。比如权责不明确与管理混乱，以及安全管理制度不完善等，都会引起管理安全风险的产生。如果责权不明确和管理较为混乱，便会使部分员工和管理人员带外来人员进入到重要区域，从而造成重要的信息数据泄露，但是并没有完善的管理制度限制，容易引起安全风险问题产生。另外网络受到攻击与威胁后，并没有采取实时监控的方式，导致无法及时预警，便难以做出有效的应对，危害到网络的安全性。同时安全风险事故发生后，无法对攻击黑客的信息收集，从而缺乏网络可控性和可审查性，很难做到有效的安全风险预防。这便需要对站点的访问活动开展多次记录，对非法入侵行为及时发现与解决。相关部门还应该根据实际的情况，建立完善的网络安全机制，并且落实到网络的各环节，然后再制定出有效的解决方案，因此需要推动管理制度与解决方案结合，从源头杜绝安全风险的产生，有利于构建出安全性较高的网络环境。

6 电力网络信息系统的安全风险应对策略

6.1 物理层

在构建网络的过程中，应该对网络的结构与布线，以及路由器和网桥的设置选择进行全面分析，然后再对重要的网络设施加强，以此保证网络的安全性较高，能够有效抵抗黑客的入侵与攻击。

6.2 网络层

电力网络信息系统想要实现不同类型的隔离，就必须要实行有效的隔离措施，如电力调度数据网络与综合信息网络，以及因特网等进行物理隔离，可以降低各网络漏洞的产生。相关部门需要对电力网络结构的边界进行识别，对不重要的网络接口断开，能够防止多样性的网络接口存在，然后再对重要的网络结构开展安全保护工作，可以保证电力网络信息系统的安全性较高。

6.3 系统层

相关部门应该采取安全等级较高的网络操作系统，如系统等级应该达到 C2，虽然等级仅有两条安全措施，并且距离较高的安全等级存在很大差距，但是具有基本的安全防范效

果，可以起到良好的预防效果。同时利用合理设置电力系统网络设施，以及主机系统配置与服务的形式，能够降低安全漏洞的出现，并且系统检测性能较高强，可以发现与解决漏洞问题，而且可以做到及时安装与升级系统缺乏的补丁，不断加强系统的安全性。

6.4 应用层

由于用户 ID 和口令认证具有较多不安全因素，所以很容易被黑客盗取，这便会给系统带来较大的安全隐患，所以便需要根据内部与外部的信息系统情况，建立统一的认证与授权机制，可以对不同的用户信息访问人员进行识别，有利于避免不法人员的入侵。想要建立安全性较高的口令，便应该保证口令的长度与复杂性较高，提高口令的猜测难度与盗取难度。此外需要做好备份和恢复工作，对重要的信息数据与应用系统备份，防止数据信息出现损坏与系统崩溃的现象发生，可以提高信息数据与系统的可用性。而且对重要的主机设备与网络设备进行备份，能够提高系统的可靠性。对实时控制系统与电力系统，应该在具备良好条件的状况下备份，保证电力系统各项业务有序开展。

6.5 管理层

电力企业想要安全实施各项业务，就必须要构建出完善的组织保证体系，并落实到企业的各环节。同时企业应该具备专业性较高的人才队伍，才能对企业状况进行分析，并且掌握先进的信息安全技术，形成专业性的管理队伍，从而有效面对出现的安全风险，这也是电力网络信息系统安全性的有效措施。

结语

电力网络信息系统在物理层、网络层、系统层、应用层、管理层等方面都具有安全风险，而且环节出现安全风险后，不仅会给电力企业信息安全带来较多隐患问题，还降低了群众的用电体验，间接地限制了电力企业的可持续发展。因此电力企业应该认识到安全风险的重要性，然后再加大对电力网络信息系统安全分线的研究，从而制定出科学合理的安全风险解决方案，营造出安全性较高的电力系统环境，有助于提高群众的用电体验，推动电力企业的可持续发展。

参考文献

[1]任丽红,刘宝擘,马博坤.电力系统网络信息安全风险防范措施分析[J].通信电源技术,2024,41(3):70-72

[2]张娟.电力网络信息系统的安全风险分析[J].中文科技期刊数据库（全文版）经济管理,2016(7):60-66

[3]罗建东.电力信息系统的网络安全技术分析[J].集成电路应用,2024,41(2):144-145

[4]赵雨.电力企业信息网络安全风险分析及防御策略研究[J].信息产业报道,2023(6):103-105

[5]李祯.电力信息通信系统网络安全防护研究[J].中国设备工程,2024(1):249-251

[6]高利达,张颖,张钦雪.电力系统通信网络的信息安全与防护机制研究[J].通信电源技术,2024,41(7):150-152

[7]王梦铃.电力系统信息通信网络安全防护研究[J].通信电源技术,2024,41(6):155-157

[8]吴先虎.电力系统网络信息安全风险防范措施研究[J].中国科技期刊数据库 工业A,2023(6):4-7