第 6 卷◆第 10 期◆版本 1.0◆2024 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

煤炭企业网络安全防护路径研究

刘宇星
中能电力科技开发有限公司
DOI：10.12238/ems.v6i10.9335

[摘　要] 在信息技术飞速发展、信息化与工业化、物联网等领域迅速结合的背景下，煤炭企业在实现智能化进程中，对网络安全的关注也日益增加。为此，煤炭企业必须对网络的安全问题给予更多的关注，以确保网络平台的最大效用，进而推动公司的发展。要想保障煤炭企业的稳定发展，就必须强化网络安全保护。本文以网络安全作为切入点，对当前煤炭企业经营过程中出现的网络安全问题进行了分析，并对提高煤炭企业网络安全保护的途径进行了探讨，以保证煤炭企业能够安全稳定地发展。
[关键词] 煤炭企业；网络安全；危险因素；防护路径

Research on the Network Security Protection Path of Coal Enterprises

Liu Yuxing
Zhongneng Electric Power Technology Development Co., Ltd

[Abstract] Against the backdrop of rapid development of information technology, integration of informatization and industrialization, and the Internet of Things, coal enterprises are paying increasing attention to network security in the process of achieving intelligence. Therefore, coal enterprises must pay more attention to network security issues to ensure the maximum effectiveness of network platforms and promote the development of the company. To ensure the stable development of coal enterprises, it is necessary to strengthen network security protection. This article takes network security as the starting point, analyzes the network security issues that arise in the current operation process of coal enterprises, and explores ways to improve the network security protection of coal enterprises to ensure their safe and stable development.
[Keywords] coal enterprises; Network security; Risk factors; Protection Path

1引言

随着新时期的到来，我国的计算机科技也进入了一个飞速发展的时期，它已广泛应用于各行各业，极大地促进了社会的发展。在中国的煤炭企业中，信息化管理得到了广泛的应用，它被运用到了生产和管理的每一个方面，使得煤炭企业的生产和管理的质量和效率都得到了极大的提升。现在，全国的煤炭企业都已经实现了生产、管理的信息化。伴随着网络安全事故的频发，以及网络攻击手段的日益增多，煤炭企业的管理者们需要对这个问题给予足够的关注，并主动地采取相应的对策，加强公司的网络系统的安全性，健全权限管理体系，保证一个煤炭企业能够平稳地发展，充分发挥其在煤炭企业中的作用。

2网络安全概述

在信息化进程中，做好网络安全保护已成为当今社会发

展的一个重要课题。网络安全就是在对网络的利用过程中，确保信息的完整性、实用性和安全性。这就意味着，在一个方面，它是指网络的硬件安全。我们将持续地引入新的电脑安全科技，并对电脑网络的安全性进行持续的革新和改进。另一方面，也要防止一些人为蓄意的破坏，例如，黑客们利用这些弱点实施非法的攻击，以谋取私利，从而导致严重的后果。

网络是让每一个单独的网路使用者能够自由沟通与通讯，达到资讯资源的共用。在煤炭企业的网络化运作过程中，其特征在于：首先，它可以对数据进行分解和集成，把煤炭企业的市场经营数据信息进行资源整合，从而提升了煤炭的节约管理的效率，为煤炭企业的发展打下了坚实的基础。二是在多个系统上实现资源的交换，从而达到资源的共享。

3煤炭企业网络安全问题

3.1 煤炭企业边界物理隔离缺失

由于缺少有效的物理隔离，企业的内部网和外界的因特网直接连接起来，给可能的网络攻击打开了方便之门。一旦被入侵，就有可能造成生产数据泄漏、控制系统被非法操纵等严重后果，对煤炭生产安全、生产效率甚至经济效益产生重大影响。所以，要保证煤炭企业的网络安全，促进煤炭工业的健康发展，就必须要强化边境的物理隔离，建立多层次的防护系统。

3.2 外部黑客入侵

黑客们通过在网络上安装的安全缺陷，侵入了公司的内部网，并且在没有得到许可的时候，还可以非法地侵入公司的核心内部网络。修改系统数据，非法获取公司机密，扰乱网络秩序。

3.3 系统自身安全漏洞

在煤炭企业的网络运营过程中，由于其系统本身的缺陷，相应的保护措施也不完善，致使黑客可以通过各种技术方法侵入煤炭企业的内网，实施违法行为。出现这种情况的根本原因，是由于煤炭企业的网络系统管理者对网络的安全性缺乏足够的关注，没有及时地升级和修补系统，导致了煤炭企业的网络系统的安全性不高，从而给了恶意攻击人员可乘之机。

4煤炭企业网络安全防护路径

4.1 工控区域物理隔离

工业控制领域的物理隔离是煤炭企业信息安全的重要组成部分。由于工业控制系统与煤炭采掘、运输、加工等关键领域的生产效率与安全性直接相关，因此对其信息安全的保护显得尤为重要。物理隔离是工业控制领域最重要的一道防御，其目标是通过物理方法将工业控制区域网络与外部网络（包括 Internet 及其它非关键网络）彻底隔绝，以防止黑客、病毒等外来入侵。

要实现工业控制区域的物理隔离，首先要从网络结构的设计开始，保证工业控制系统的独立工作，并且不与其它的网络有直接的联系。同时，要强化对物理设备的控制，比如使用专门的网闸、单项隔离等设备，并对其进行限制，避免未经授权的用户对其进行修改或者在其内部植入恶意代码。另外，对设备的物理隔离设备也要进行定期的检测与维修，以保证它在任何时候都是有效的。通过这些措施，煤炭企业可以明显地提高工业控制系统的网络安全保护水平，保证了生产流程的顺利运转，保证了安全、可靠的数据。

4.2 白名单防病毒安全策略

在工控系统中，通过对操作员站、工程师站、服务器和客户端的“白名单”机制，为工控系统添加可信应用，构建一个安全可靠的应用运行环境。在运行的终端和主机上，都应该采用经过了检测和验证的主机安全软件，并且只有经过用户公司认证和审核的软件才能上线使用。针对工控系统中的工作终端和主机，采用病毒库扫描、原始代码审计等方法，构建了工控系统的防毒、防病毒及恶意软件的入侵管理机制。设定工控区的系统组态列表，根据需要对网络边界，主机终端，控制设备执行必要的审核。在系统结构发生重大变化时，需要对其进行相应的修改，并对其造成的影响进行分析，并在部署之前对其进行必要的网络安全检查；在工业控制范围内，及时地更新系统，如果在一些重要的系统中发生了网络安全问题，那么就应该立即下线，并在更新系统补丁之前，对这个补丁进行必要的网络安全检查。

4.3 数字签名身份认证

在煤炭生产经营过程中，实施网上办公已是今后的发展方向。所谓的数字签名，就是只能由发送者生成，而不能被其他人使用，这是一种在用户浏览用户信息时，需要进行信

息核实的方式。在信息服务、合同签署等方面，都要求顾客在数字签名操作平台上签字，检查数字签名和保留的信息，验证使用者资料的真伪，从而提高煤炭公司的合作效率。

4.4 加强关键设备配置策略

在煤炭企业的信息安全保障系统中，必须强化核心设备的配置战略。服务器、防火墙和交换机是网络架构中的关键部件，它们的安全配置对整体网络的安全性有很大的影响。煤炭企业需要对其进行全方位的安全防护，以确保其能够有效地抵抗网络攻击，维护其核心财产。针对这些问题，本文提出了一种新的解决方案，即：在服务器上采用强口令和多因子认证等方法来阻止非授权用户的访问；在防火墙上设置规范，保证只让必需的数据流通过，并在此基础上实时更新防火墙中的威胁智能库，以应付不断出现的网络威胁；通过对交换机的 VLAN 划分，使网络数据流在逻辑上被隔离，从而降低了广播风暴的发生以及可能存在的安全隐患。另外，还要对重要设备进行定期的安全性审核，以及对系统的脆弱性进行检测，以便能够及时地发现和解决存在的安全问题，以保证设备的安全运行。采取上述措施后，煤炭企业的网络安全保护水平得到了明显的提高，为企业的安全生产和运营管理提供了可靠的保证。

4.4 数据加密安全防护

在煤炭企业的信息安全管理中，信息加密是一个必不可少的环节。随着煤炭企业信息化建设的不断深入，海量的生产经营、客户、财务等敏感数据都会通过互联网进行传递与存储，这些数据一旦泄漏或被篡改，将给企业带来难以估量的损失。为此，对数据进行加密保护就显得非常重要。

数据加密技术可以把明文信息转化成非授权方无法读取和使用的密文，从而保证了数据的保密性、完整性和可用性。对于煤炭企业来说，需要根据不同的数据类型、不同的服务场景，选择合适的加密算法与加密方法，例如对称加密、不对称加密、哈希加密等，来实现对特定信息的加密。与此同时，构建一套完整的密钥管理系统，保证密钥在产生、保存、分发、使用和销毁过程中均满足安全性要求，避免密钥的泄漏和滥用。

另外，在煤炭企业中，要加强对数据加密技术的培训与运用，增强工作人员对数据加密的重视程度，保证数据加密政策的有效实施。通过对数据加密的安全防护措施的执行，可以有效地减少数据泄漏和篡改的危险，对公司的核心财产和顾客的隐私进行了保护，为公司的可持续发展提供了强有力的保证。

4.5 加强网络安全技术人才的培养

随着社会的发展，网路科技的发展，网路安全防范的技术也随之提升。所以，要从源头上预防和控制网络信息安全事件的发生，就需要在科技上进行投资，并对其进行培训。要持续地对电脑网络安全技术进行研究与更新，增强煤炭公司工作人员对网络安全的保护意识，并主动地为其举办一次网络安全教育课程，将网络安全的相关知识进行普及，并对各类网络安全事件作出反应。

5结论

当前，煤炭企业控制区域内的信息安全保护仍是煤炭安全工作中的一个薄弱环节。本文根据实际工作中遇到的问题，归纳了影响煤炭企业网络安全的各种因素，为煤炭企业提供了有效的保护手段。目前，煤炭企业迫切需要进行的防护工作包括专用通信、等保建设、工业隔离区建设和网络安全管理系统建设。推动“智慧矿山”网络的“全矿”建设，全面提高“智慧”建设进程中的网络、终端、通信、应用等全方位的“全方位”防御能力，让“智慧矿山”的网络安全防护体系建设具有一致性和合规性。

[参考文献]

[1]弓会龙，高一洪.基于大数据的主动防御技术在煤炭企业网络安全中的应用研究[J].中国高新科技，2024，(11)：83-85.

[2]王峰，侯锬.探索煤炭企业工控网络安全防护与预测方法[J].内蒙古煤炭经济，2024，(05)：119-121.

[3]弓会龙，高梓轩.网络安全态势感知平台在煤炭企业中的应用研究[J].中国高新科技，2024，(01)：45-47.

[4]原生芾，侯尚武，侯振堂，等.大型煤炭企业网络信息安全体系建设实践[J].软件，2023，44（07）：160-163.

[5]刘燕.关于煤炭企业网络安全技术的研究与应用[J].能源技术与管理，2022，47（06）：189-192.