文章编号:1671-251X(2021)S2-0165-03

浅谈煤炭企业网络安全防护

吴昊天

(国能信息技术有限公司,北京 100000)

摘要:给出了造成煤炭企业网络信息不安全的 4 个因素:自然灾害、黑客入侵、系统病毒及自身漏洞。阐述了煤炭企业网络安全防护内容切实有效的做好专网建设、等保建设、工业隔离区建设与网络安全管理体系建设的防护工作,实现智能矿山网络安全防护建设的一致性、合规性:① 在重点网络区域与其他网络区域之间设置安全隔离区,并采用单向隔离技术手段阻断生产控制层与生产管理层之间直接的网络连接和数据访问;② 将工业控制系统中的可信应用程序加入到白名单列表中,形成安全可信的应用程序运行环境;③ 对关键主机设备、网络设备、控制组件等进行冗余配置,提供重要数据的本地数据备份与恢复功能、重要数据处理系统的热冗余;④ 在工业主机登录、应用服务资源访问、工业云平台访问等过程中使用身份认证管理;⑤ 选择背景可信、技术过硬的网络安全服务队伍;⑥ 在工控区域中安装工业入侵检测系统、部署网络安全应急预案;⑦ 机房部署在防震、防风和防雨的建筑内;⑧ 明确网络安全管理责任人,落实网络安全责任制。

关键词:煤炭企业网络安全;煤炭智能化;网络安全防护;工业隔离区

中图分类号:TD672 文献标志码:A

Discussion on network security protection of coal enterprises

WU Haotian

(Guoneng Information Technology Co., Ltd., Beijing 100000, China)

0 引言

随着信息技术的不断发展,信息化与工业化及物联网技术快速融合[1-4],给煤矿生产带来新的发展机遇,2016 年国家安全生产监督管理总局印发了《煤矿安全监控系统升级改造技术方案》通知,明确要求了进一步提高煤矿安全监控系统的数字化和信息化水平,保障监控系统的信息准确性和实时性。从初期的信息传递,到建立安全生产、调度和管理的网络信息系统[5],再到如今的煤矿智能化,计算机网络给煤炭企业的生产带来便捷的同时,也带来了潜在的危险。如果网络系统出现问题,不仅会给煤炭企业用户带来经济损失,还会造成个人信息的泄露,更为严重的是导致整个网络系统陷入瘫痪[6]。在煤炭企业智能化的过程中,网络安全越来越受到煤炭企业的重视。因此,煤炭企业要更加重视网络安全建设,以保证发挥网络平台最大功效,从而更有效地促进企业发展[7]。

1 煤炭企业网络安全问题

煤炭企业所需网络环境一般包括企业内部网络、外部互联网和企业广域网,各类应用和控制系统在其中部署方式及传输线路较为复杂。在网络环境下,煤炭企业网络信息不安全的因素主要来自以下几个方面。

(1) 自然灾害。在网络运行期间,影响网络安全的自然灾害主要包括硬件设备设施故障,机房水患、失火、雷电等引发的设备失效,从而造成核心数据丢失和应用程序服务停止等[8]。

(2) 黑客入侵。黑客利用煤矿部署在互联网系统的安全漏洞,入侵到企业内网,并通过内网在未经允许的情况下非法进入企业核心内部网络系统[9-11],对系统进行数据修改、非法取得企业机密、破坏网络秩序。

(3) 系统病毒。病毒通过用户使用网络、电子邮件、U 盘及未经授权软件等被带入煤矿企业的网络环境[12],在企业内网络设备间进行传播,破坏操作系统、应用系统及设备硬件,短时间内便会造成计

收稿日期:2021-06-24;编辑:郑海霞。

作者简介:吴昊天(1995—),男,北京人,网络与信息安全工程师,主要从事工控网络与信息安全工作,E-mail:20035110@chnenergy.com.cn。

算机系统或应用软件的瘫痪。

(4) 自身漏洞。应用系统自身存在漏洞和缺陷是导致病毒及黑客攻击煤炭企业网络的主要原因[13]。病毒和黑客能够入侵到煤炭企业内部系统中,主要是因为煤炭企业网络信息安全措施不完善、不到位;系统管理员的疏忽导致补丁程序未被及时安装,方便了病毒和黑客利用这些漏洞侵入内部系统,造成严重后果。

2 煤炭企业网络安全防护

煤炭企业网络安全防护工作应按照"垂直分层、水平分区、边界管控、主机监控、内部审评、统筹管理"的纵深防御思路,实现智能矿山网络安全防护全矿井覆盖。

(1) 边界隔离与访问控制。煤矿工业控制系统与企业办公相关系统进行网络区域划分,并对各网络区域进行地址分派,防止重点网络区域被规划在边界范围[14],在重点网络区域与其他网络区域之间设置安全隔离区,并采用单向隔离技术手段(工业防火墙[15]、网闸等)实现物理隔离,阻断生产控制层与生产管理层之间直接的网络连接和数据访问。

遵循合理的访问控制策略,在无特殊情况下,除允许正常访问外,管控端口拒绝向互联网开放HTTP、FTP、Telnet 等高危常用网络服务的行为;确需远程访问的,应以单向安全加固的访问控制为策略进行数据安全防护,对访问持续时间进行管控,并选用加标锁定策略;确需远程维护的,选用VPN[16]等远程连接方式进行。

对用户访问工业控制系统操作过程完成网络安全审计,并保存常用类型日志 6 个月以上。

(2) 软件与配置的安全管控。在工业控制系统中,采用白名单机制对操作员站、工程师站、服务器与客户机进行主机加固,将工业控制系统中的可信应用程序加入到白名单列表中,形成安全可信的应用程序运行环境。工作的终端与主机上都应使用通过测试环境中检验测试合格的主机安全软件,只有被使用企业唯一授权和审计过的软件允许上线使用。建立防病毒和恶意软件入侵管理机制,对工业控制系统中的工作终端与主机进行病毒库扫描、原代码审计[17]等防护手段。

设置工控区域系统配置清单并按要求对网络边界、主机终端、控制设备进行必要审计。当发生较大配置改变时,应部署相应变更机制,并分析影响范围,该配置变更部署前要开展必要的网络安全检测;及时对工控区域内的系统进行补丁升级,当关键系统出现网络安全故障时,应第一时间进行下线升级,系统补丁升级前,要对该补丁开展必要的网络安全检测[18]。

(3) 数据与资产安全。对缓存数据库和主数据库中的关键工业控制数据进行定期备份,对关键工业控制设备 PLC 进行系统升级、程序下载等操作时进行程序备份;对关键主机设备、网络设备、控制组件等进行冗余配置,提供重要数据的本地数据备份与恢复功能、重要数据处理系统的热冗余,以保证系统的高可用性。

(4) 身份认证。在工业主机登录、应用服务资源访问、工业云平台访问等过程中使用身份认证[19-20]管理。对于关键设备、系统和平台应采用口令、密码技术、证书、生物识别等 1 种以上的鉴别技术进行身份鉴别。

使用最低权限规则划分用户权限,对于默认用户应修改名称或删除,默认用户的口令必须更改为强口令;提高工控类设备、PLC 控制软件、通信类设备等的登录用户名及口令的复杂度,禁止设置默认口令或简单口令,要按时对口令进行修改;加强对身份认证证书信息保护力度。

(5) 供应链管理。在选择网络安全防护规划、设计、建设、运维或评估等服务商时,优先考虑背景可信、技术过硬的网络安全服务队伍。以保密协议的方式要求服务商做好保密工作,防范敏感信息外泄。

(6) 安全监控和应急预案演练。在工控区域中安装工业入侵检测系统,以快速检测到网络安全攻击或非法行为。

部署网络安全应急预案,以保障网络安全受到威胁时工控区域整体网络安全态势正常运行;定期对工控区域内的系统进行紧急响应演习,对于不当或不足的事件处理方案进行有效修改;快速开展必要的防护措施,在避免事件规模升级的基础上,保护现场以便后期调查。

(7) 物理和环境安全防护。机房应选择在具有防震、防风和防雨的建筑内部署。将各类机柜、设施和设备等通过接地系统安全接地,选取静电隔离材质的地面、采用静电消除器、佩戴防静电手环等防止静电的产生;设置防雷保安器或过电压保护装置防止感应雷;对调度机房管理进行划分区域,电源线和通信电缆隔离敷设,避免互相干扰,在区域之间设置隔离防火措施。

对工控区域内的主机终端,应禁止开放所有外接接口。如若必须使用,可通过 USB 锁等外接设备

网络安全防护方法进行必要的访问控制。

(8) 落实责任。通过建立网络安全管理机制、成立网络安全领导小组等方式,明确网络安全管理责任人,落实网络安全责任制。

3　结语

目前,煤炭行业工业控制区的网络安全防护仍然是煤矿安全薄弱环节。结合实践经验,对危害煤炭企业网络安全的因素进行了总结,并提出了煤炭企业网络安全防护措施。切实有效的做好专网建设、等保建设、工业隔离区建设与网络安全管理体系建设是当下煤炭企业急需开展的防护工作。推进智能矿山网络安全防护全矿井覆盖工作,整体提升煤矿在智能化建设过程中的网络、终端、通信、应用等方面的综合防御能力,实现智能矿山网络安全防护建设的一致性、合规性。

参考文献:

[1] 胡权.我国煤矿安全监测监控系统发展与应用[J].煤炭科技,2017(3):202-204.

[2] 闫兆振.煤矿安全监控多系统融合平台[J].工矿自动化,2017,43(2):11-14.

[3] 王启峰.煤矿安全监控多系统井下融合方法[J].工矿自动化,2017,43(2):7-10.

[4] 丁恩杰,金雷,陈迪.互联网+感知矿山安全监控系统研究[J].煤炭科学技术,2017,45(1):129-134.

[5] 何同林,冯丹.煤炭企业网络信息安全问题分析及对策探讨[J].矿业安全与环保,2007(3):66-68.

[6] 秦文明.网络环境下煤炭企业信息安全及防护探析[J].煤炭技术,2013,32(3):249-251.

[7] 吴兆法.煤炭企业网络安全解决方案[J].山西煤炭管理干部学院学报,2014,27(4):35-37.

[8] 杨宝霖.浅析煤炭企业网络安全建设和管理[J].信息系统工程,2012(4):76-77.

[9] 刘迎.工业智能化引发新的安全挑战[J].信息安全与通信保密,2015(2):56-57.

[10] 张帆,管增伦.煤炭企业信息网络安全和管理策略浅析[J].中国煤炭,2006(2):47-48.

[11] 龚俭,臧小东,苏琪,等.网络安全态势感知综述[J].软件学报,2017,28(4):1010-1026.

[12] 赵保贤,王金灿.煤炭企业网络安全与发展规划浅谈[J].陕西煤炭,2017,36(6):59-63.

[13] 马友友.基于智能化技术构建的网络安全管理模式[J].网络安全技术与应用,2015(1):103-104.

[14] 吴海君.煤炭企业网络安全建设和管理初探[J].信息安全与通信保密,2007(11):92-94.

[15] 张龙旗.大型煤炭企业网络安全分析及对策[J].山东煤炭科技,2007(4):49-50.

[16] 林秋珍,朱玲玲,石记红,等.基于 VPN 技术的煤炭企业安全生产信息网络的构建与优化[J].中州煤炭,2010(1):34-36.

[17] 顾闯.煤炭企业工控网络安全防护与预测方法研究[J].煤炭科学技术,2019,47(11):143-147.

[18] 刘永军.关于煤炭企业网络信息安全问题分析及对策探究[J].科技创新与应用,2014(19):70.

[19] 魏凤鸣.煤炭企业网络安全探讨[J].煤,2003(1):57-58.

[20] 李岩.煤炭企业网络信息安全管理措施[J].信息通信,2015(6):144.