包钢企业网络安全体系的探索与实践*

刘仲厅,段春明,乌 晨

(包头钢铁(集团)有限责任公司信息服务中心,内蒙古 包头 014010)

摘 要: 文章针对网络安全的实质和目标,根据我国网络安全现状和国内外信息安全标准,探索建立符合包钢企业网络安全管理体系的理论框架。

关键词: 企业网络; 网络安全; 防护体系; 管理方法

中图分类号: TP393.08 **文献标识码**: B **文章编号**: 1009-5438(2021)04-0086-03

DOI:10.13647/j.cnki.btgkj.2021.04.022

Exploration and Practices on Enterprise Network Security System of Baotou Steel

Liu Zhong-ting, Duan Chun-ming, Wu Chen

(*Information Service Center of Baotou Iron & Steel (Group) Co., Ltd., Baotou* 014010, *Inner Mongolia Autonomous Region, China*)

Abstract: In the paper, the establishment of theoretical framework in line with the enterprise network security management system of Baotou Steel is explored according to network security status in our country as well as information security standards at home and abroad aiming at essence and target of network security.

Key words: enterprise network; network security; protection system; management method

包钢网络经过十多年的建设已形成了集数据、语音、视频三网合一功能的企业园区信息网络。网络承载着公司的ERP系统、协同办公系统、视频会议系统、门禁考勤等重要的业务系统,各分子公司接入单位50余家,终端接入电脑上万台。作为一个大型钢铁企业,公司的生产和网络及各大业务系统息息相关,密不可分。伴随《网络安全法》的正式颁布和实施,网络安全工作进入有法可依、有法必依的阶段,对网络安全的重视程度已经上升到国家层面,习近平总书记在全国网络安全和信息化工作会议上强调,“没有网络安全就没有国家安全,就没有经济社会稳定运行,广大人民群众利益也难以得到保障”。包钢的信息化发展不断壮大,敏感信息、网络安全成为企业信息化发展面临的突出问题。如何构建一个安全可靠的企业网络安全系统也成为企业领导人面临的重要问题。

依照2019年5月13号发布的等保2.0的三个关键标准GB/T 22239—2019《信息安全技术网络安全等级保护基本要求》,GB/T 25070—2019《信息安全技术网络安全等级保护安全设计要求》和GB/T 28448—2019《信息安全技术网络安全等级保护测评要求》,充分结合包钢(集团)公司当前网络信息情况,转变安全合规理念,从“被动防御”演进至“综合防御、纵深防御、主动防御”。经过多年的信息化建设,逐步形成了具有自己企业特点的一套网络安全防护体系。

* **收稿日期**: 2021-03-30

作者简介: 刘仲厅(1976-),男,内蒙古包头市人,工程师,现从事网络管理工作。

1　建立网络安全体系

包钢(集团)公司网络安全是根据分区分域防护的原则,按照一个中心三重防护的思想,建设符合三级等保的信息系统保护深度防御体系。

按照信息系统业务处理过程将系统划分成安全计算环境、安全区域边界和安全通信网络三部分,以计算节点为基础对这三部分实施保护,构成由安全管理中心支撑下的计算环境安全、区域边界安全、通信网络安全所组成的“一个中心,三重防护”结构。

1.1　安全管理中心

通过采用态势感知平台构建统一的信息安全管理平台[1],态势感知的关键是通过采集和分析大量分散的安全设备提供的安全事件,并将这些信息以可视化的方式呈现出来,从而使网络管理者能够迅速把握复杂、动态的安全态势。

(1) 采集防火墙、入侵检测日志、网络日志、主机日志及漏洞信息,对多种设备的日志数据进行统一格式。

(2) 支持海量设备日志存储,符合等级保护对日志保留的要求,通过流量探针、沙箱、防火墙及入侵防御设备的协同工作,关联多个安全设备的安全事件信息,从整体上反映网络安全状态,并对网络安全的发展趋势进行预测和预警,手动或自动联动 FW 设备或者 IPS 设备,进行黑名单的下发和阻断策略的配置,并能够在 FW 设备或 IPS 设备上成功阻断恶意访问。

(3) 通过安全威胁情报中心感知网络状态、受攻击情况、攻击来源,制定有预见性的应急预案,做好相应防范准备[2]。

(4) 通过流量探针进行流量分析,展示通过网络原始流量分析异常流量事件数量,包括异常流量事件总数、高危事件总数、中危事件总数、低危事件总数。

1.2　安全区域边界

通过业务类型进行网络区域划分,划分 LCA 云资源区、ERP 资源区、DMZ 资源区,各区域通过防火墙进行安全隔离防护。

互联网及 DMZ 出口采用防火墙、入侵防御、行为管理等安全设备进行边界防护,对边界进行恶意代码防范、入侵威胁防御及上网行为控制管理,对网络中的攻击行为,包括病毒、蠕虫、木马、间谍软件等进行有效防御。

DMZ 区部署了 Web 应用防火墙,提供 Web 应用漏洞扫描功能,检测 Web 应用程序是否存在 SQL 注入、跨站脚本漏洞。对黑客入侵行为、SQL 注入/跨站脚本等各类 Web 应用攻击、DDoS 攻击进行有效检测、阻断及防护。

1.3　安全计算环境

主机部署杀毒软件,对主机系统进行恶意代码防护,通过统一的管理平台进行代码升级和监控。

部署堡垒机对设备的使用者进行身份鉴别,并对权限进行控制,防止非法登录,对登录访问的行为进行记录,做到行为的溯源。

部署数据审计对数据库中数据操作行为进行审计,避免受到恶意数据删除、修改等行为。

部署漏洞扫描,定期对主机、网络、数据库、Web 进行漏洞检测,并给出修复建议,及时对安全漏洞进行修复。

部署数据备份系统,对业务数据进行周期性备份,保护数据安全性。

1.4　安全通信网络

对外连接采用 SSL VPN、IPSec VPN 等加密技术对通信链路进行加密,增强网络传输的安全性。各设备间通过防火墙建立安全访问策略,DMZ 与内网进行安全隔离。

2　合理布局网络拓扑结构

包钢网络拓扑结构是星型结构,其显著特点是结构简单,便于管理,便于建网;网络延迟时间较小,传输误差较低。目前在厂区以光缆方式接入公司网络的有 36 家单位,光缆敷设总长度达 80 km 以上,以运营商专线方式接入的有 14 家单位。各单位根据业务划分 VLAN,并且分配相应的 IP 地址。严格控制同一广播域内通讯的主机数量,保障网络的高可用和高性能。在实际网络运行中,这种规划使网络攻击者实施攻击的难度增加,而网络管理中由于终端的范围细化,可采取的手段增多。

3　提升网络安全意识

在强化物理技术防护企业网络安全和员工行为的同时,还需加强企业网络管理的制度建设,应制定严格的上网行为管理办法,通过制度去约束员工在互联网上的行为。管理与技术手段结合在企业中要营造良好的网络文化氛围,使员工自觉良好地应用网络为工作服务。要提高全体员工的个人素质和敬

业精神,使员工自觉维护企业的名誉和利益。此外要培养员工的网络安全意识与网络安全防护能力。

4 结束语

有效的技术手段是网络安全的基础工作,但仅靠网络安全技术是绝对无法确保信息安全的。只有建立严格的网络安全管理制度,才能充分发挥网络安全技术的效能,才能使网络信息更加安全可靠。只有不断对网络安全体系进行深入的研究、探讨和完善,才能更好地实现网络安全,保证包钢企业信息化建设的正常进行。

参 考 文 献

[1] 张强. 网络安全态势评估与预测技术研究[D]. 哈尔滨:哈尔滨工程大学,2010.

[2] 杨义先,钮心忻. 网络安全理论与技术[M]. 北京:人民邮电出版社,2003.

中文名称	英文	含义
国际蒸汽表卡	I. T. calorie; calrt	热量的非法定计量单位,为4.186 8焦耳。
国际烛光	international candle; bi	发光强度的非法定计量单位,为1.02坎德拉。
毫英寸	millinch; thou; mil; min	长度的英制单位,为25.4微米。
华氏度	degree Fahrenherit; °F	温度的非法定计量单位,换算较复杂:x华氏度为(5/9)(x + 459.67)开尔文,或者x华氏度为(5/9)(x - 32)摄氏度。
加仑	gallon; gal	体积、容积的英制单位,为4.546 09立方分米(英)或3.785 41立方分米(美)。
斤[1]		“市斤”的异名。
斤[2]		“司马斤”的异名。
金衡盎司	troy ounce; oz tr; ozt	质量的英制单位,用于贵金属,为31.103 5克。
净吨	net ton	“英吨”为907.185千克时的异名之一,与“短吨”相同。
居里	curie; Ci	放射性活度的旧单位,为37 000 000 000贝可勒尔。
卡	cal	热量的非法定计量单位,为4.185 5焦耳(15 ℃卡)或4.181 6焦耳(20 ℃卡)。
卡路里	calorie	“卡”的异名。
克拉		“米制克拉”的异名。
兰氏度	degree Rankine; °R	热力学温度的英制单位,为5/9开尔文。