浅谈唐安煤矿网络安全预案建设

秦志刚

（山西兰花科技创业股份有限公司唐安煤矿分公司）

摘　要：当前，网络空间安全形势日益严峻，我国的政府机构、大中型企业的门户网站和专网重要核心业务系统常常成为攻击者的主要攻击目标，为妥善处理和应对唐安煤矿关键信息基础设施可能发生的网络与信息安全突发事件，确保信息基础设施、信息监控系统以及办公门户网站的安全、稳定、持续运行，防止给煤矿或相关部门造成重大影响和经济损失，避免因单个受害点影响全域网络安全的稳定性，需进一步加强网络安全与信息化应急保障能力，网络安全应急预案是安全防护的一道重要防线，是及早发现、及时处置、全面调度至关重要的应急措施。本文对唐安煤矿网络安全应急预案提出了建设构想。

关键词：网络安全；应急预案；设计

1　前　言

随着信息化系统在唐安煤矿的逐步应用，目前在煤炭专网上以及矿局域网上安装运行的系统越来越多，近年来，我市发生了多次网络安全事件，唐安煤矿部分信息系统也不同程度的出现网络安全小事件，给煤矿各类安全生产信息系统安全、稳定运行带来了严重影响。

2　唐安煤矿网络安全应急预案总体设计

2.1 应急预案适用范围

本预案适用于山西兰花科技创业股份有限公司唐安煤矿分公司由于人为原因（病毒、恶意程序、非法程序、非法远程访问）、软硬 件缺陷或故障、自然灾害等原因严重影响到信息系统的正常运行，出现系统中断、系统破坏、数据破坏或者国家、企业秘密信息被窃取、泄露等，导致在国家安全、社会稳定、生产安全、企业利益等方面造 成重大危害，危及信

息安全的紧急事件。

2.2应急预案的实施主体

唐安煤矿网络安全应急预案的实施主体就是负责领导、制定、组织实施应急预案的工作人员，即唐安煤矿网络与信息安全突发事件应急响应领导组。负责网络与信息安全事件应急建设管理和应急处置。

2.3应急预案的客体

唐安煤矿网络安全应急预案的客体就是网络信息应急处理的对象，即针对何种事件进行应急处置，由于不同的应急事件给唐安煤矿网络带来的危害不同，对唐安煤矿正常工作带来的影响也不同，因而要做好唐安煤矿网络安全的防范和伊宁及工作，首先要在应急预案中将唐安煤矿面临的应急事件按相应等级进行分类。

2.3.1唐安煤矿网络信息应急事件的种类

网络与信息安全事件分为有害程序事件、网络攻击事件、信息破 坏事件、信息内容安全事件、设备设施故障、灾害性事件及其他事件。

(1)有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木 马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件 和其他有害程序事件。

(2)网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏 洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网 络攻击事件。

(3)信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

(4)信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会 稳定和公众利益的事件。

(5)设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

(6)灾害性事件是指由自然灾害等其他突发事件导致的网络与 信息安全事件。

(7)其它类事件：指不能归为以上 6 类的信息安全突发事件。

2.3.2唐安煤矿网络信息应急事件的级别设定

按照网络与信息安全突发情况影响范围、系统损失和社会影响，分为四级：特别重大、重大、较大、一般。

(1)唐安煤矿重大网络与信息事件

此类事件是指唐安煤矿重要网络和信息系统遭受特别严重的系统损失，造成系统 大面积瘫痪，丧失业务处理能力，致使煤矿安全生产和正常经营长时间无法恢复的。

(2)唐安煤矿重大网络与信息事件

此类事件是指唐安煤矿重要网络和信息系统遭受特别严重的系统损失，造成系统 大面积瘫痪，丧失业务处理能力。

(3)唐安煤矿较大网络与信息事件

此类事件是指唐安煤矿重要网络和信息系统中单个办公信息系统无法向互联网公众、相关业务科室提供正常的应用服务，导致煤矿正常经营活动受到重大影响的；单个重要信息系统发生网络安全突发事件导致煤矿无法正常进行安全生产活动，需停产撤人的；(如：安全监控系统、重大设备监 测系统、供电监测系统)。

(4)唐安煤矿一般网络与信息事件

此类事件是指唐安煤矿重要网络和信息系统中由于自然灾害、人为原因、软硬件缺陷或故障等，导致煤矿出现系统无法正常提供服务的，且经应急处置小组及日常运行小组评 估，预计在 1 小时以内可以恢复的。对煤矿企业形象和网络稳定造成 较小影响。

3 唐安煤矿网络安全预案的方案设计

3.1 应急预警的方案设计

预警信息包括事件的类别、预警级别、起始时间、可能影响范围、警示事项应采取的措施和时限要求、发布机关等。对于可能发生网络与信息安全突发事件，应急处置小组应立即采取措施控制事态，并进行风险评估，判定事件等级并向领导组汇报，申请发布预警。领导组接到汇报后应立即组织现场救援，查明事件状态及原因，及时对信息进行技术分析、研判，根据问题的性质、危害程度，提出安全预警级别。领导组在发布事件预警时，明确预警的响应范围和公开程度（或保密要求）。领导组在发布事件预警后，应通过电话等方式，将预警尽快传达到相关部门和人员。

3.2 应急处置的方案设计

当接到各级网络信息安全突发事件通知后，由网络信息安全应急领导组组长宣布启动本预案。

3.2.1 应急处置方案启动

唐安煤矿发生网络与信息安全突发事件后，应急办立即向领导组汇报，根据领导组指示下发启动本预案的指令。各小组按照各自职责开始实施应急处置并及时报送信息。

3.2.2 应急处置程序的设计

（1）控制事态防止蔓延。应急处置小组在技术专家小组支持指导下立即采取各种技术措施、管控手段，最大限度阻止和控制事态蔓延。

（2）消除隐患恢复系统。应急办组织各小组根据事件发生原因，针对性制定解决方案，备份数据、保护设备、排查隐患等。对业务连续性要求高的受破坏网络与信息系统要及时组织恢复。

（3）调查取证。应急处置小组及技术专家小组在屏幕截图、现场拍照、导出日志等相关证据的基础上，开展问题定位和溯源追踪工作。积极配合集团、县、市相关主管单位开展调查取证工作。

（4）在处置中需要协调其他更高层次技术及工作支持的，由领导组根据实际，报请上级主管部门，协调技术人员支持。

（5）次生事件处置。对于引发或可能引发其他安全事件的，综合协调小组应及时按程序上报。

4 结束语

近年来，随着信息化的深入发展，智能控制、远程控制采集、数字化办公、多网多系统融合、智慧化矿山建设等新技术逐步展现、新系统增多。网络信息安全的重要性不言而喻，对于信息安全的认知也跨出了一大步，网络安全应急预案建设成了唐安煤矿的首要任务。建设好网络应急预案要明确适用范围、要完善应急预警和应急处置机制，从而构建一个高效、安全的网络系统，确保唐安煤矿各类系统一旦发生危害事件能及时处理，保证唐安煤矿各信息化系统稳定运行，为矿山发展保驾护航。