四川省水利厅

川水函〔2021〕577号

四川省水利厅
关于做好网络安全联防联控工作的通知

厅机关各处室、厅直属各单位、各市(州)水利(水务)局、大型水利工程管理单位:

根据《网络安全法》有关规定,公安部于近期开展了2021年度网络安全攻防演练。为配合做好公安部网络安全攻防演练,及时发现水利行业网络安全漏洞和隐患,检验水利行业网络安全联防联控机制。经厅领导同意,现就有关事项通知如下:

一、提高政治站位,压实主体责任

2021年是中国共产党建党100周年,做好今年的网络安全保

障工作具有特殊意义,全省水利行业要把网络安全作为落实意识形态工作责任制的重要内容,时刻紧绷网络安全意识形态这根弦,从严从细从实抓好网络安全风险防控相关工作,织密网络安全防护网,为庆祝建党100周年营造风清气正的水利网络环境。各单位要高度重视此次网络安全攻防演练,将网络安全防守和水利行业联防联控工作纳入重点工作予以研究部署,落实好网络安全保障工作,切实履行网络安全工作主体责任,认真贯彻落实《网络安全法》和《四川省水利网络安全管理办法实施细则(试行)》、《四川省水利厅网络与信息安全综合应急预案(试行)》。按照“谁主管谁负责、谁建设谁负责、谁运行谁负责、谁使用谁负责”的原则,各单位网络安全直接责任人为本单位演练工作负责人,负责抓好本单位和下级单位攻防演练和联防联控机制落实,市(州)要负责抓好县级及以下部门的协同防守和问题整改落实,把责任落实到具体部门、岗位和个人,做到领导到位、责任到位、机构到位、人员到位、经费到位和措施到位。

二、聚焦突出问题,强化工作举措

3月15日至28日,水利部开展了以目标系统为标靶,不限制攻击路径,以防汛骨干网、防汛决策指挥系统、水资源管理系统(包括地下水)、工业控制系统、门户网站、VPN、电子邮箱、手机APP、互联网与业务网边界等为重点演练目标进行攻击测试的网络安全攻防演练,我省7个系统被攻陷,其中弱口令问题较为突出,另外存在部分信息系统Struts2文件老旧,信息设备病毒库、系统漏洞补丁更新不及时,系统源代码管理不到位等风险隐患。各

有关单位要在水利部网络安全攻防演练基础上,强化问题导向,开展网络安全自查工作,抓好现有问题整改落实,补足水利信息化发展工作短板,坚决守住网络安全底线。针对公安部2021年度网络安全攻防演练要重点做好如下工作:

一是组建技术工作专班。演练期间,各单位要及时抽调专业技术力量组成工作专班,继续执行24小时值班值守制度,在现有技术防护基础上充分利用监测系统和设备,加强本单位信息系统监测预警,以安全监测为核心,以各类安全防护设备为辅助,特别是水利部、长江委延伸系统和防汛骨干网部署系统,要实时监测各类安全攻击和事件,协同各部门、各单位及厂商共享情报,合作开展全方位协同防护,从监测、预警、分析、验证、研判、处置和溯源实施闭环防守工作,阻断攻击源,确保及时、准确发现和处置问题。

二是梳理老旧信息资产。抓紧梳理本单位老旧信息资产情况,及时关停未使用服务器、网络端口和“僵尸系统”,更新服务器系统补丁、加强访问控制、设置访问白名单。明确各系统、设备的主管单位、运行单位,明确职责划分,依据资产清单,在安全合规的基础上,梳理互联网暴露面及网络边界弱点,减少情报、文档泄露,把攻击面缩到最小,特别是曾经被发现或通报的问题隐患要确保整改到位。

三是强化联防联控机制。各单位要全程做好与水利厅信息中心的情报共享、协同联动,演练期间时刻关注“四川水利行业网络安全工作群”qq群(群号:785729751),及时共享自行监测或厂商提供的网络攻击、中高危漏洞等威胁情报,及时封禁各类情报提供

的IP地址和研判、处置涉及本单位的安全事件,对监测到的攻击或疑似攻击及时留存防守处置证据,认真填写《防守报告》(见附件)并于三小时内通过OA系统报送至厅信息中心,做到“一处预警、处处设防,一项整改、处处处置”。

四是做好日常防护工作。各单位要确保安装防火墙及防病毒软件,及时更新病毒特征库,并且定期进行信息设备的病毒查杀、漏洞修复及补丁升级工作,严格杜绝信息系统弱口令问题,加强数据备份管理,补全网络安全设备,在打开移动储存器前用杀毒软件进行检查,加强边界防护,加固各类信息系统,限制访问IP,对VPN进行密切监测,留意各种异常警告并及时修复。同时,要强化广大干部职工网络安全防范意识,不打开来历不明的网页、邮箱或短信中的链接,不随意扫码,不轻信浏览网页时弹出的“支付风险、垃圾清理、漏洞风险”等信息,定期更换信息设备及信息系统用户密码、清理敏感数据,用户终端管理做到下班人走关机。

三、坚持举一反三,强化问题整改

各单位要抓住两次实战攻防演练契机,及时总结分析,以演练结果为数据支撑,总结分析联防联控中存在的问题及原因,结合日常工作,完善工作机制,制定持续整改计划,落实具体时间、经费、责任部门及人员,确保守住水利网络安全防线。特别是要总结2020年公安厅和2021年水利部攻防演练中出现的问题,针对问题,解决问题,尽快形成整体联防联控态势。

四、其他有关要求

(一)为实现攻防演练目标,确保演练顺利开展,攻防演练期

间防守方各单位不允许针对演练活动采取如下极端的防守应对措施:平时正常运行系统在演练期间做下线处理;停用参演系统部分或全部功能,或替换为纯静态页面;大量或整段封禁 IP;不遵从演练指挥部调度安排;以及造成演练无法顺利进行的其他影响演练正常开展的过度防守行为。

(二)演练过程中,各单位要严格落实安全保密措施,筛选政治可靠人员参演并全员签署保密协议。未经演练水利部攻防演练指挥部同意,不得向外界公布演练相关内容,严禁在互联网及其他公开渠道发表、传播涉演练活动信息;演练过程中加强实时监测,严防敌对势力、不法分子借机进行网络攻击窃密和渗透破坏。

联 系 人:王培瑾

联系方式:028-60595955,15198032663

附件:防守报告模板

四川省水利厅

2021 年 4 月 15 日

附件

防守报告

<table>
<tr><td>*目标系统名称</td><td></td></tr>
<tr><td>*目标 URL</td><td></td></tr>
<tr><td>*目标系统 IP</td><td></td></tr>
<tr><td>*网络层级</td><td>☐互联网　☐办公网　☐业务内网　☐生产网</td></tr>
<tr><td>*攻击 IP</td><td>（请输入攻击 IP，多个 IP 空格或换行分隔）</td></tr>
<tr><td>攻击手段</td><td></td></tr>
<tr><td>*防御手段</td><td></td></tr>
<tr><td>*防御类型</td><td>1. 发现类
☐发现 webshell 木马、主机木马
数量：
☐发现账号异常，并采取处置措施
普通用户应用层，数量：
普通用户系统层，数量：
普通用户数据库，数量：
普通用户网络设备，数量：
管理员应用层，数量：
管理员系统层，数量：
管理员数据库，数量：
管理员网络设备，数量：
☐发现恶意邮件（包含恶意链接、病毒邮件）
数量：
2. 消除类
☐处置现场接触式攻击
数量：
☐处置攻击者进入互联网区事件
数量：
☐处置攻击者进入逻辑隔离业务内网区事件
数量：
☐处置攻击者进入生产网区事件
数量：
3. 应急处置
☐应急处置能力，数量：
（请输入说明，长度不超过 100 个字符）
4. 追踪溯源
☐完整还原攻击链条，溯源到黑客的虚拟身份、真实身份，溯源到攻击队员，反控攻击主机，根据程度阶梯给分。
数量：
（请输入说明，长度不超过 100 个字符）</td></tr>
<tr><td>*防御过程描述：</td><td>（请分步骤描述防御过程，对每步的关键防御手段必须给出清晰描述并配图说明，以便裁判审核打分。）</td></tr>
</table>

信息公开选项:依申请公开

四川省水利厅办公室　　2021 年 4 月 15 日印发